United Nations A/CN.9/493

General Assembly

Distr.: General
17 May 2001

Original: English

United Nations Commission
on International Trade Law
Thirty-fourth session
Vienna, 25 June - 13 July 2001

Electronic Signatures

Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures

Note by the Secretariat

1. Pursuant to decisions taken by the Commission at its twenty-ninth (1996) [1] and thirtieth (1997) [2] sessions, the Working Group on Electronic Commerce devoted its thirty-first to thirty-seventh sessions to the preparation of the draft UNCITRAL Model Law on Electronic Signatures (hereinafter referred to as "the Model Law", "the draft Model Law" or "the new Model Law"). Reports of those sessions are found in documents A/CN.9/437, 446, 454, 457, 465, 467 and 483. In preparing the Model Law, the Working Group noted that it would be useful to provide in a commentary additional information concerning the Model Law. Following the approach taken in the preparation of the UNCITRAL Model Law on Electronic Commerce, there was general support for a suggestion that the new Model Law should be accompanied by a guide to assist States in enacting and applying that Model Law. The guide, much of which could be drawn from the *travaux préparatoires* of the Model Law, would also be helpful to other users of the Model Law.

2. At its thirty-seventh session (Vienna, September 2000), the Working Group completed the preparation of the draft articles of the Model Law and discussed the draft guide to enactment on the basis of a note by the Secretariat (A/CN.9/WG.IV/WP.86 and Add.1). The Secretariat was requested to prepare a revised version of the draft guide reflecting the decisions made by the Working Group, based on the various views, suggestions and concerns that had been expressed at the thirty-seventh session. Due to lack of time, the Working Group did not complete its deliberations regarding the draft guide to enactment (see A/CN.9/483, paras. 23 and 145-152). It was agreed that some time should be set aside by the Working Group at its thirty-eighth session for completion of that agenda item. It was noted that the draft Model Law, together with the draft guide to enactment, would be submitted to the Commission for review and adoption at its thirty-fourth session, to be held at Vienna from 25 June to 13 July 2001.

3. At its thirty-eighth session (New York, March 2001), the Working Group reviewed the draft guide to enactment of the UNCITRAL Model Law on Electronic Signatures, based on a revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.88). The deliberations and decisions of the Working Group with respect to the draft guide are reflected in the report of that session (A/CN.9/484). The Secretariat was requested to prepare a revised version of the guide, based on those deliberations and decisions (A/CN.9/484, para. 19). The revised version of the draft guide prepared by the Secretariat is annexed to this note.

V.01-84085

Annex

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES

WITH

GUIDE TO ENACTMENT

2001

CONTENTS

General Assembly Resolution .....

Part One

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

Page

Article 1. Sphere of application 5
Article 2. Definitions 5
Article 3. Equal treatment of signature technologies 6
Article 4. Interpretation 6
Article 5. Variation by agreement 6
Article 6. Compliance with a requirement for a signature 6
Article 7. Satisfaction of article 6 7
Article 8. Conduct of the signatory 7
Article 9. Conduct of the certification service provider 7
Article 10. Trustworthiness 8
Article 11. Conduct of the relying party 9
Article 12. Recognition of foreign certificates and electronic signatures 9

Part Two

GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

Paragraphs *Page*

Purpose of this Guide 1-2 10

Chapter I. Introduction to the Model Law 3-85 10

I. PURPOSE AND ORIGIN OF THE MODEL LAW 3-25 10

A. Purpose 3-5 10
B. Background 6-11 11
C. History 12-25 13

II. THE MODEL LAW AS A TOOL FOR HARMONIZING LAWS 26-28 16

III.	GENERAL REMARKS ON ELECTRONIC SIGNATURES		29-62	17
	A.	Functions of signatures	29-30	17
	B.	Digital signatures and other electronic signatures	31-62	17
		1. Electronic signatures relying on techniques other than public-key cryptography	33-34	18
		2. Digital signatures relying on public-key cryptography	35-62	18
		(a) Technical notions and terminology	36-44	18
		(i) Cryptography	36-37	18
		(ii) Public and private keys	38-39	19
		(iii) Hash function	40	19
		(iv) Digital signature	41-42	20
		(v) Verification of digital signature	43-44	20
		(b) Public key infrastructure (PKI) and certification service provider	45-61	20
		(i) Public key infrastructure (PKI)	50-52	21
		(ii) Certification service provider	53-61	22
		(c) Summary of the digital signature process	62	24
IV.	MAIN FEATURES OF THE MODEL LAW		63-82	25
	A.	Legislative nature of the Model Law	63-64	25
	B.	Relationship with the UNCITRAL Model Law on Electronic Commerce	65-68	25
		1. New Model Law as a separate legal instrument	65	25
		2. New Model Law fully consistent with the UNCITRAL Model Law on Electronic Commerce	66-67	26
		3. Relationship with article 7 of the UNCITRAL Model Law on Electronic Commerce	68	26
	C.	"Framework" rules to be supplemented by technical regulations and contract	69-70	27
	D.	Added certainty as to the legal effects of electronic signatures	71-76	27
	E.	Basic rules of conduct for the parties involved	77-81	29
	F.	A technology-neutral framework	82	30
	G.	Non-discrimination of foreign electronic signatures	83	30
V.	ASSISTANCE FROM THE UNCITRAL SECRETARIAT		84-86	30
	A.	Assistance in drafting legislation	84-85	30
	B.	Information on the interpretation of legislation based on the Model Law	86	31
Chapter II.	**Article-by-article remarks**		87-160	31
Title			87	31
Article 1.	Sphere of application		88-92	31
Article 2.	Definitions		93-106	33
Article 3.	Equal treatment of signature technologies		107	37
Article 4.	Interpretation		108-110	38
Article 5.	Variation by agreement		111-114	39
Article 6.	Compliance with a requirement for a signature		115-131	40
Article 7.	Satisfaction of article 6		132-136	44
Article 8.	Conduct of the signatory		137-141	46
Article 9.	Conduct of the certification service provider		142-146	48
Article 10.	Trustworthiness		147	50
Article 11.	Conduct of the relying party		148-151	51
Article 12.	Recognition of foreign certificates and electronic signatures		152-160	52

Part One

UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

(as approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000)

Article 1. Sphere of application

This Law applies where electronic signatures are used in the context* of commercial** activities. It does not override any rule of law intended for the protection of consumers.

* The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies where electronic signatures are used, except in the following situations: [...]."

** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 (1) or otherwise meets the requirements of applicable law.

Article 4. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Article 6. Compliance with a requirement for a signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Paragraph (3) does not limit the ability of any person:

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

(5) The provisions of this article do not apply to the following: [...]

Article 7. Satisfaction of article 6

(1) [Any person, organ or authority, whether public or private, specified by the enacting State as competent] may determine which electronic signatures satisfy the provisions of article 6.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

(3) Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) the signatory knows that the signature creation data have been compromised; or
(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

(2) A signatory shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 9. Conduct of the certification service provider

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

(i) the identity of the certification service provider;
(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) the method used to identify the signatory;
(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
(iii) that the signature creation data are valid and have not been compromised;
(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;
(v) whether means exist for the signatory to give notice pursuant to article 8 (1) (b);
(vi) whether a timely revocation service is offered;

(e) where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8(1)(b) and, where services under subparagraph d (vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 10. Trustworthiness

For the purposes of article 9(1)(f), in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and
(ii) observe any limitation with respect to the certificate.

Article 12. Recognition of foreign certificates and electronic signatures

(1) In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had to:

(a) the geographic location where the certificate is issued or the electronic signature created or used; or

(b) the geographic location of the place of business of the issuer or signatory.

(2) A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(4) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

(5) Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

Part Two

GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001)

Purpose of this Guide

1. In preparing and adopting the UNCITRAL Model Law on Electronic Signatures (also referred to in this publication as "the Model Law" or "the new Model Law"), the United Nations Commission on International Trade Law (UNCITRAL) was mindful that the Model Law would be a more effective tool for States modernizing their legislation if background and explanatory information were provided to executive branches of Governments and legislators to assist them in using the Model Law. The Commission was also aware of the likelihood that the Model Law would be used in a number of States with limited familiarity with the type of communication techniques considered in the Model Law. This Guide, much of which is drawn from the *travaux préparatoires* of the Model Law, is also intended to be helpful to other users of the text, such as judges, arbitrators, practitioners and academics. Such information might also assist States in considering which, if any, of the provisions should be varied in order to be adapted to any particular national circumstances necessitating such variation. In the preparation of the Model Law, it was assumed that the Model Law would be accompanied by such a guide. For example, it was decided in respect of a number of issues not to settle them in the Model Law but to address them in the Guide so as to provide guidance to States enacting the Model Law. The information presented in this Guide is intended to explain why the provisions in the Model Law have been included as essential basic features of a statutory device designed to achieve the objectives of the Model Law.

2. The present Guide to Enactment has been prepared by the Secretariat pursuant to the request of UNCITRAL made at the close of its thirty-fourth session, in 2001. It is based on the deliberations and decisions of the Commission at that session,[8] when the Model Law was adopted, as well as on considerations of the Working Group on Electronic Commerce, which conducted the preparatory work.

Chapter I. Introduction to the Model Law

I. PURPOSE AND ORIGIN OF THE MODEL LAW

A. Purpose

3. The increased use of electronic authentication techniques as substitutes for hand-written signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as "electronic signatures"). The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international

phenomenon, where legal harmony as well as technical interoperability is a desirable objective.

4. Building on the fundamental principles underlying article 7 of the UNCITRAL Model Law on Electronic Commerce (always referred to in this publication under its full title to avoid confusion) with respect to the fulfilment of the signature function in an electronic environment, this new Model Law is designed to assist States in establishing a modern, harmonized and fair legislative framework to address more effectively the issues of electronic signatures. In a modest but significant addition to the UNCITRAL Model Law on Electronic Commerce, the new Model Law offers practical standards against which the technical reliability of electronic signatures may be measured. In addition, the Model Law provides a linkage between such technical reliability and the legal effectiveness that may be expected from a given electronic signature. The Model Law adds substantially to the UNCITRAL Model Law on Electronic Commerce by adopting an approach under which the legal effectiveness of a given electronic signature technique may be pre-determined (or assessed prior to being actually used). The Model Law is thus intended to foster the understanding of electronic signatures, and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions. Moreover, by establishing with appropriate flexibility a set of basic rules of conduct for the various parties that may become involved in the use of electronic signatures (i.e., signatories, relying parties and third-party certification service providers) the Model Law may assist in shaping more harmonious commercial practices in cyberspace.

5. The objectives of the Model Law, which include enabling or facilitating the use of electronic signatures and providing equal treatment to users of paper-based documentation and users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law (and also the provisions of the UNCITRAL Model Law on Electronic Commerce) in its national legislation for those situations where parties opt to use electronic means of communication, an enacting State would appropriately create a media-neutral environment. The media-neutral approach also used in the UNCITRAL Model Law on Electronic Commerce is intended to provide in principle for the coverage of all factual situations where information is generated, stored or communicated, irrespective of the medium on which such information may be affixed (see Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, para. 24). The words "a media-neutral environment", as used in the UNCITRAL Model Law on Electronic Commerce, reflect the principle of non-discrimination between information supported by a paper medium and information communicated or stored electronically. The new Model Law equally reflects the principle that no discrimination should be made among the various techniques that may be used to communicate or store information electronically, a principle that is often referred to as "technology neutrality" (A/CN.9/484, para. 23).

B. Background

6. The Model Law constitutes a new step in a series of international instruments adopted by UNCITRAL, which are either specifically focused on the needs of electronic commerce or were prepared bearing in mind the needs of modern means of communication. In the first category, specific instruments geared to electronic commerce comprise the Legal Guide on Electronic Funds Transfers (1987), the UNCITRAL Model Law on International Credit Transfers (1992) and the UNCITRAL Model Law on Electronic Commerce (1996 and 1998). The second category consists of all international conventions and other legislative instruments adopted by UNCITRAL since 1978, all of which promote reduced formalism and contain definitions of

"writing" that are meant to encompass de-materialized communications.

7. The best known UNCITRAL instrument in the field of electronic commerce is the UNCITRAL Model Law on Electronic Commerce. Its preparation in the early 1990s resulted from the increased use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions. It was realized that new technologies had been developing rapidly and would develop further as technical supports such as information highways and the Internet became more widely accessible. However, the communication of legally significant information in the form of paperless messages was hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. With a view to facilitating the increased use of modern means of communication, UNCITRAL has prepared the UNCITRAL Model Law on Electronic Commerce. The purpose of the UNCITRAL Model Law on Electronic Commerce is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce".

8. The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that, in a number of countries, the existing legislation governing communication and storage of information was inadequate or outdated because it did not contemplate the use of electronic commerce. In certain cases, existing legislation still imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents. With respect to the notions of "written", "signed" and "original" documents, the UNCITRAL Model Law on Electronic Commerce adopted an approach based on functional equivalence. The "functional equivalent approach" is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions can be fulfilled through electronic-commerce techniques (see Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, paras. 15-18).

9. At the time when the UNCITRAL Model Law on Electronic Commerce was being prepared, a few countries had adopted specific provisions to deal with certain aspects of electronic commerce. However, there existed no legislation dealing with electronic commerce as a whole. This could result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Moreover, while sound laws and practices were necessary in all countries where the use of electronic data interchange (EDI) and electronic mail was becoming widespread, this need was also felt in many countries with respect to such communication techniques as telecopy and telex. Under article 2(b) of the UNCITRAL Model Law on Electronic Commerce, EDI is defined as "the electronic transfer from computer to computer of information using an agreed standard to structure the information".

10. The UNCITRAL Model Law on Electronic Commerce also helped to remedy disadvantages that stemmed from the fact that inadequate legislation at the national level created obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. To a large extent, disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may still contribute to limiting the extent to which businesses may access international markets.

11. Furthermore, at an international level, the UNCITRAL Model Law on Electronic Commerce may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of

electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those States parties to such international instruments, the adoption of the UNCITRAL Model Law on Electronic Commerce as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

C. History

12. After adopting the UNCITRAL Model Law on Electronic Commerce, the Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [3]

13. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). The Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of legislation in that area. While no firm decision as to the form and content of such work had been reached, the Working Group had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157). The Commission endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities.

14. With respect to the exact scope and form of the uniform rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the uniform rules should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce. Thus, the uniform rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the uniform rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought. [4]

15. The Working Group began the preparation of the uniform rules (to be adopted later as the Model Law) at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73).

16. At its thirty-first session (1998), the Commission had before it the report of the Working Group on the work of its thirty-second session (A/CN.9/446). It was noted that the Working Group, throughout its thirty-first and thirty-second sessions, had experienced manifest difficulties in reaching a common understanding of the new legal issues that arose from the increased use of digital and other electronic signatures. It was also noted that a consensus was still to be found as to how those issues might be addressed in an internationally acceptable legal framework. However, it was generally felt by the Commission that the progress realized so far indicated that the uniform rules were progressively being shaped into a workable structure.

17. The Commission reaffirmed the decision made at its thirtieth session as to the feasibility of preparing such uniform rules and expressed its confidence that more progress could be accomplished by the Working Group at its thirty-third session on the basis of the revised draft prepared by the Secretariat (A/CN.9/WG.IV/WP.76). In the context of that discussion, the Commission noted with satisfaction that the Working Group had become generally recognized as a particularly important international forum for the exchange of views regarding the legal issues of electronic commerce and for the preparation of solutions to those issues. [5]

18. The Working Group continued revision of the uniform rules at its thirty-third session (1998) and thirty-fourth session (1999) on the basis of notes prepared by the Secretariat (A/CN.9/WG.IV/WP.76 and A/CN.9/WG.IV/WP.79 and 80). The reports of the sessions are contained in documents A/CN.9/454 and 457.

19. At its thirty-second session (1999), the Commission had before it the report of the Working Group on those two sessions (A/CN.9/454 and 457). The Commission expressed its appreciation for the efforts accomplished by the Working Group in its preparation of the uniform rules. While it was generally agreed that significant progress had been made at those sessions in the understanding of the legal issues of electronic signatures, it was also felt that the Working Group had been faced with difficulties in the building of a consensus as to the legislative policy on which the uniform rules should be based.

20. A view was expressed that the approach currently taken by the Working Group did not sufficiently reflect the business need for flexibility in the use of electronic signatures and other authentication techniques. As currently envisaged by the Working Group, the uniform rules placed excessive emphasis on digital signature techniques and, within the sphere of digital signatures, on a specific application involving third-party certification. Accordingly, it was suggested that work on electronic signatures by the Working Group should either be limited to the legal issues of cross-border certification or be postponed altogether until market practices were better established. A related view expressed was that, for the purposes of international trade, most of the legal issues arising from the use of electronic signatures had already been solved in the UNCITRAL Model Law on Electronic Commerce (see below, para. 28). While regulation dealing with certain uses of electronic signatures might be needed outside the scope of commercial law, the Working Group should not become involved in any such regulatory activity.

21. The widely prevailing view was that the Working Group should pursue its task on the basis of its original mandate. With respect to the need for uniform rules on electronic signatures, it was explained that, in many countries, guidance from UNCITRAL was expected by governmental and legislative authorities that were in the process of preparing legislation on electronic signature issues, including the establishment of public-key infrastructures (PKI) or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by the Working Group to

focus on PKI issues and PKI terminology, it was recalled that the interplay of relationships between three distinct types of parties (i.e., signatories, certification authorities and relying parties) corresponded to one possible PKI model, but that other models were conceivable, e.g., where no independent certification service provider was involved. One of the main benefits to be drawn from focusing on PKI issues was to facilitate the structuring of the uniform rules by reference to three functions (or roles) with respect to key pairs, namely, the key issuer (or subscriber) function, the certification function, and the relying function. It was generally agreed that those three functions were common to all PKI models. It was also agreed that those three functions should be dealt with irrespective of whether they were in fact served by three separate entities or whether two of those functions were served by the same person (e.g., where the certification service provider was also a relying party). In addition, it was widely felt that focusing on the functions typical of PKI and not on any specific model might make it easier to develop a fully media-neutral rule at a later stage (ibid., para. 68).

22. After discussion, the Commission reaffirmed its earlier decisions as to the feasibility of preparing such uniform rules and expressed its confidence that more progress could be accomplished by the Working Group at its forthcoming sessions. [6]

23. The Working Group continued its work at its thirty-fifth (September 1999) and thirty-sixth (February 2000) sessions on the basis of notes prepared by the Secretariat (A/CN.9/WG.IV/WP. 82 and 84). At its thirty-third (2000) session, the Commission had before it the report of the Working Group on the work of those two sessions (A/CN.9/465 and 467). It was noted that the Working Group, at its thirty-sixth session, had adopted the text of draft articles 1 and 3 to 12 of the uniform rules. It was stated that some issues remained to be clarified as a result of the decision by the Working Group to delete the notion of enhanced electronic signature from the uniform rules. A concern was expressed that, depending on the decisions to be made by the Working Group with respect to draft articles 2 and 13, the remainder of the draft provisions might need to be revisited to avoid creating a situation where the standard set forth by the uniform rules would apply equally to electronic signatures that ensured a high level of security and to low-value certificates that might be used in the context of electronic communications that were not intended to carry significant legal effect.

24. After discussion, the Commission expressed its appreciation for the efforts extended by the Working Group and the progress achieved in the preparation of the uniform rules. The Working Group was urged to complete its work with respect to the uniform rules at its thirty-seventh session and to review the draft guide to enactment to be prepared by the Secretariat.[7]

25. The Working Group completed the preparation of the uniform rules at its thirty-seventh (September 2000) session. The report of that session is contained in document A/CN.9/483. The Working Group also discussed the draft guide to enactment. The Secretariat was requested to prepare a revised version of the draft guide reflecting the decisions made by the Working Group, based on the various views, suggestions and concerns that had been expressed at the current session. Due to lack of time, the Working Group did not complete its deliberations regarding the draft guide to enactment. It was agreed that some time should be set aside by the Working Group at its thirty-eighth session for completion of that agenda item. It was noted that the uniform rules (in the form of a draft UNCITRAL Model Law on Electronic Signatures), together with the draft guide to enactment, would be submitted to the Commission for review and adoption at its thirty-fourth (2001) session. *[Note by the Secretariat: this section recording the history of the Model Law is to be completed after final consideration and adoption of the Model Law by the Commission].*

II. THE MODEL LAW AS A TOOL FOR HARMONIZING LAWS

26. As the UNCITRAL Model Law on Electronic Commerce, the new Model Law is in the form of a legislative text that is recommended to States for incorporation into their national law. The Model Law is not intended to interfere with the normal operation of the rules of private international law (see below, para. 136). Unlike an international convention, model legislation does not require the State enacting it to notify the United Nations or other States that may have also enacted it. However, States are strongly encouraged to inform the UNCITRAL Secretariat of any enactment of the new Model Law (or any other model law resulting from the work of UNCITRAL).

27. In incorporating the text of the model legislation into its legal system, a State may modify or leave out some of its provisions. In the case of a convention, the possibility of changes being made to the uniform text by the States parties (normally referred to as "reservations") is much more restricted; in particular trade law conventions usually either totally prohibit reservations or allow only very few, specified ones. The flexibility inherent in model legislation is particularly desirable in those cases where it is likely that the State would wish to make various modifications to the uniform text before it would be ready to enact it as national law. Some modifications may be expected in particular when the uniform text is closely related to the national court and procedural system. This, however, also means that the degree of, and certainty about, harmonization achieved through model legislation is likely to be lower than in the case of a convention. However, this relative disadvantage of model legislation may be balanced by the fact that the number of States enacting model legislation is likely to be higher than the number of States adhering to a convention. In order to achieve a satisfactory degree of harmonization and certainty, it is recommended that States make as few changes as possible in incorporating the new Model Law into their legal systems, and that they take due regard of its basic principles, including technology neutrality, non-discrimination between domestic and foreign electronic signatures, party autonomy and the international origin of the Model Law. In general, in enacting the new Model Law (or the UNCITRAL Model Law on Electronic Commerce), it is advisable to adhere as much as possible to the uniform text in order to make the national law as transparent and familiar as possible for foreign users of the national law.

28. It should be noted that some countries consider that the legal issues related to the use of electronic signatures have already been solved by the UNCITRAL Model Law on Electronic Commerce, and do not plan on adopting further rules on electronic signatures until market practices in this new area are better established. However, States enacting the new Model Law alongside the UNCITRAL Model Law on Electronic Commerce may expect additional benefits. For those countries where governmental and legislative authorities are in the process of preparing legislation on electronic signature issues, including the establishment of public-key infrastructures (PKI), certain provisions of the Model Law offer the guidance of an international instrument that was prepared with PKI issues and PKI terminology in mind. For all countries, the Model Law offers a set of basic rules that can be applied beyond the PKI model, since they envisage the interplay of two distinct functions that are involved in any type of electronic signature (i.e., creating and relying on an electronic signature), and a third function involved in certain types of electronic signatures (i.e., certifying an electronic signature). Those three functions should be dealt with irrespective of whether they are in fact served by three or more separate entities (e.g., where various aspects of the certification function are shared between different entities) or whether two of those functions are served by the same person (e.g., where the certification function is served by a relying party). The Model Law thus provides common grounds for PKI systems relying on independent certification authorities and electronic signature systems where

no such independent third party is involved in the electronic signature process. In all cases, the new Model Law provides added certainty regarding the legal effectiveness of electronic signatures, without limiting the availability of the flexible criterion embodied in article 7 of the UNCITRAL Model Law on Electronic Commerce (see below, paras. 67 and 70 to 75).

III. GENERAL REMARKS ON ELECTRONIC SIGNATURES [8]

A. Functions of signatures

29. Article 7 of the UNCITRAL Model Law on Electronic Commerce is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the UNCITRAL Model Law on Electronic Commerce, the Working Group discussed the following functions traditionally performed by hand-written signatures: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed. For example, a signature might attest to: the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing); the intent of a person to associate itself with the content of a document written by someone else; the fact that, and the time when, a person had been at a given place. The relationship of the new Model Law with article 7 of the UNCITRAL Model Law on Electronic Commerce is further discussed below, in paragraphs 65, 67 and 70 to 75 of this Guide.

30. In an electronic environment, the original of a message is indistinguishable from a copy, bears no hand-written signature, and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection, and the speed of processing multiple transactions. The purpose of various techniques currently available on the market or still under development is to offer the technical means by which some or all of the functions identified as characteristic of hand-written signatures can be performed in an electronic environment. Such techniques may be referred to broadly as "electronic signatures".

B. Digital signatures and other electronic signatures

31. In discussing the desirability and feasibility of preparing the new Model Law, and in defining the scope of uniform rules on electronic signatures, UNCITRAL has examined various electronic signature techniques currently being used or still under development. The common purpose of those techniques is to provide functional equivalents to (1) hand-written signatures; and (2) other kinds of authentication mechanisms used in a paper-based environment (e.g., seals or stamps). The same techniques may perform additional functions in the sphere of electronic commerce, which are derived from the functions of a signature but correspond to no strict equivalent in a paper-based environment.

32. As indicated above (see paras. 21 and 28), guidance from UNCITRAL is expected in many countries, by governmental and legislative authorities that are in the process of preparing legislation on electronic signature issues, including the establishment of public key infrastructures (PKI) or other projects on closely related matters (see A/CN.9/457, para. 16). As to the decision made by UNCITRAL to focus on PKI issues and PKI terminology, it should be noted that the interplay of relationships between three distinct types of parties (i.e., signatories, suppliers of certification

services and relying parties) corresponds to one possible PKI model, but other models are already commonly used in the marketplace (e.g., where no independent certification service provider is involved). One of the main benefits to be drawn from focusing on PKI issues was to facilitate the structuring of the Model Law by reference to three functions (or roles) with respect to electronic signatures, namely, the signatory function, the certification function, and the relying function. Two of those functions are common to all PKI models (i.e., creating and relying on an electronic signature). The third function is involved in many PKI models (i.e., certifying an electronic signature). Those three functions should be dealt with irrespective of whether they are in fact served by three or more separate entities (e.g., where various aspects of the certification function are shared between different entities), or whether two of those functions are served by the same person (e.g., where the certification service provider is also a relying party). Focusing on the functions performed in a PKI environment and not on any specific model also makes it easier to develop a fully media-neutral rule to the extent that similar functions are served in non-PKI electronic signature technology.

1. Electronic signatures relying on techniques other than public-key cryptography

33. Alongside "digital signatures" based on public-key cryptography, there exist various other devices, also covered in the broader notion of "electronic signature" mechanisms, which may currently be used, or considered for future use, with a view to fulfilling one or more of the above-mentioned functions of hand-written signatures. For example, certain techniques would rely on authentication through a biometric device based on hand-written signatures. In such a device, the signatory would sign manually, using a special pen, either on a computer screen or on a digital pad. The hand-written signature would then be analysed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the relying party for authentication purposes. Such an authentication system would presuppose that samples of the hand-written signature have been previously analysed and stored by the biometric device. Other techniques would involve the use of personal identification numbers (PINs), digitized versions of hand-written signatures, and other methods, such as clicking an "OK-box".

34. UNCITRAL has intended to develop uniform legislation that can facilitate the use of both digital signatures and other forms of electronic signatures. To that effect, UNCITRAL has attempted to deal with the legal issues of electronic signature issues at a level that is intermediate between the high generality of the UNCITRAL Model Law on Electronic Commerce and the specificity that might be required when dealing with a given signature technique. In any event, consistent with media neutrality in the UNCITRAL Model Law on Electronic Commerce, the new Model Law is not to be interpreted as discouraging the use of any method of electronic signature, whether already existing or to be implemented in the future.

2. Digital signatures relying on public-key cryptography [9]

35. In view of the increasing use of digital signature techniques in a number of countries, the following introduction may be of assistance.

(a) Technical notions and terminology

(i) Cryptography

36. Digital signatures are created and verified by using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and back into the original form. Digital signatures use what is known as "public key cryptography", which is often based on the use of algorithmic

functions to generate two different but mathematically-related "keys" (i.e., large numbers produced using a series of mathematical formulae applied to prime numbers). One such key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other one for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms.

37. While the use of cryptography is one of the main features of digital signatures, the mere fact that a digital signature is used to authenticate a message containing information in digital form should not be confused with a more general use of cryptography for confidentiality purposes. Confidentiality encryption is a method used for encoding an electronic communication so that only the originator and the addressee of the message will be able to read it. In a number of countries, the use of cryptography for confidentiality purposes is limited by law for reasons of public policy that may involve considerations of national defence. However, the use of cryptography for authentication purposes by producing a digital signature does not necessarily imply the use of cryptography to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message.

(ii) Public and private keys

38. The complementary keys used for digital signatures are named the "private key", which is used only by the signatory to create the digital signature, and the "public key", which is ordinarily more widely known and is used by a relying party to verify the digital signature. The user of a private key is expected to keep the private key secret. It should be noted that the individual user does not need to know the private key. Such a private key is likely to be kept on a smart card, or to be accessible through a personal identification number or through a biometric identification device, e.g., through thumbprint recognition. If many people need to verify the signatory's digital signatures, the public key must be available or distributed to all of them, for example by publication in an on-line repository or any other form of public directory where it is easily accessible. Although the keys of the pair are mathematically related, if an asymmetric cryptosystem has been designed and implemented securely it is virtually impossible to derive the private key from knowledge of the public key. The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is particularly difficult and time-consuming to determine which two prime numbers created that new, larger number. [10] Thus, although many people may know the public key of a given signatory and use it to verify that signatory's signatures, they cannot discover that signatory's private key and use it to forge digital signatures.

39. It should be noted, however, that the concept of public-key cryptography does not necessarily imply the use of the above-mentioned algorithms based on prime numbers. Other mathematical techniques are currently used or under development, such as cryptosystems relying on elliptic curves, which are often described as offering a high degree of security through the use of significantly reduced key-lengths.

(iii) Hash function

40. In addition to the generation of key pairs, another fundamental process, generally referred to as a "hash function", is used in both creating and verifying a digital signature. A hash function is a mathematical process, based on an algorithm which

creates a digital representation, or compressed form of the message, often referred to as a "message digest", or "fingerprint" of the message, in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes named a "one-way hash function", it is virtually impossible to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

(iv) Digital signature

41. To sign a document or any other item of information, the signatory first delimits precisely the borders of what is to be signed. Then a hash function in the signatory's software computes a hash result unique (for all practical purposes) to the information to be signed. The signatory's software then transforms the hash result into a digital signature using the signatory's private key. The resulting digital signature is thus unique to both the information being signed and the private key used to create the digital signature.

42. Typically, a digital signature (a digitally signed hash result of the message) is attached to the message and stored or transmitted with that message. However, it may also be sent or stored as a separate data element, as long as it maintains a reliable association with the corresponding message. Since a digital signature is unique to its message, it is inoperable if permanently disassociated from the message.

(v) Verification of digital signature

43. Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key, and whether the newly computed hash result matches the original hash result that was transformed into the digital signature during the signing process.

44. The verification software will confirm the digital signature as "verified" if: (1) the signatory's private key was used to sign digitally the message, which is known to be the case if the signatory's public key was used to verify the signature because the signatory's public key will verify only a digital signature created with the signatory's private key; and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

(b) Public key infrastructure (PKI) and suppliers of certification services

45. To verify a digital signature, the verifier must have access to the signatory's public key and have assurance that it corresponds to the signatory's private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. If public key cryptography is to serve its

intended purposes, it needs to provide a way to make keys available to a wide variety of persons, many of whom are not known to the signatory, where no relationship of trust has developed between the parties. To that effect, the parties involved must have a degree of confidence in the public and private keys being issued.

46. The requested level of confidence may exist between parties who trust each other, who have dealt with each other over a period of time, who communicate on closed systems, who operate within a closed group, or who are able to govern their dealings contractually, for example, in a trading partner agreement. In a transaction involving only two parties, each party can simply communicate (by a relatively secure channel such as a courier or telephone, with its inherent feature of voice recognition) the public key of the key pair each party will use. However, the same level of confidence may not be present when the parties deal infrequently with each other, communicate over open systems (e.g., the World Wide Web on the Internet), are not in a closed group, or do not have trading partner agreements or other law governing their relationships.

47. In addition, because public-key cryptography is a highly mathematical technology, all users must have confidence in the skill, knowledge and security arrangements of the parties issuing the public and private keys. [11]

48. A prospective signatory might issue a public statement indicating that signatures verifiable by a given public key should be treated as originating from that signatory. The form and the legal effectiveness of such a statement would be governed by the law of the enacting State. For example, a presumption of attribution of electronic signatures to a particular signatory could be established through publication of the statement in an official bulletin or in a document recognized as "authentic" by public authorities (see A/CN.9/484, para. 36). However, other parties might be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of inadvertently trusting an imposter, or of having to disprove a false denial of a digital signature (an issue often referred to in the context of "non-repudiation" of digital signatures) if a transaction should turn out to prove disadvantageous for the purported signatory.

49. One type of solution to some of these problems is the use of one or more third parties to associate an identified signatory or the signatory's name with a specific public key. That third party is generally referred to as a "certification authority", "certification service provider" or "supplier of certification services" in most technical standards and guidelines (in the Model Law, the term "certification service provider" has been chosen). In a number of countries, such certification authorities are being organized hierarchically into what is often referred to as a public key infrastructure (PKI). Other solutions may include, for example, certificates issued by relying parties.

(i) Public key infrastructure (PKI)

50. Setting up a public key infrastructure (PKI) is a way to provide confidence that: (1) a user's public key has not been tampered with and in fact corresponds to that user's private key; and (2) the cryptographic techniques being used are sound. To provide the confidence described above, a PKI may offer a number of services, including the following: (1) managing cryptographic keys used for digital signatures; (2) certifying that a public key corresponds to a private key; (3) providing keys to end users; (4) publishing a secure directory of public keys or certificates; (5) managing personal tokens (e.g., smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (6) checking the identification of end users, and providing them with services; (7) providing time-

stamping services; and (8) managing cryptographic keys used for confidentiality encryption where the use of such a technique is authorized.

51. A public key infrastructure (PKI) is often based on various hierarchical levels of authority. For example, models considered in certain countries for the establishment of possible PKIs include references to the following levels: (1) a unique "root authority", which would certify the technology and practices of all parties authorized to issue cryptographic key pairs or certificates in connection with the use of such key pairs, and would register subordinate certification authorities;[12] (2) various certification authorities, placed below the "root" authority, which would certify that a user's public key actually corresponds to that user's private key (i.e., has not been tampered with); and (3) various local registration authorities, placed below the certification authorities, and receiving requests from users for cryptographic key pairs or for certificates in connection with the use of such key pairs, requiring proof of identification and checking identities of potential users. In certain countries, it is envisaged that notaries public might act as, or support, local registration authorities.

52. The issues of PKI may not lend themselves easily to international harmonization. The organization of a PKI may involve various technical issues, as well as issues of public policy that may better be left to each individual State at the current stage.[13] In that connection, decisions may need to be made by each State considering the establishment of a PKI, for example as to: (1) the form and number of levels of authority which should be comprised in a PKI; (2) whether only certain authorities belonging to the PKI should be allowed to issue cryptographic key pairs or whether such key pairs might be issued by the users themselves; (3) whether the certification authorities certifying the validity of cryptographic key pairs should be public entities or whether private entities might act as certification authorities; (4) whether the process of allowing a given entity to act as a certification service provider should take the form of an express authorization, or "licensing", by the State, or whether other methods should be used to control the quality of certification authorities if they were allowed to operate in the absence of a specific authorization; (5) the extent to which the use of cryptography should be authorized for confidentiality purposes; and (6) whether Government authorities should have the right to gain access to encrypted information, through a mechanism of "key escrow" or otherwise. The Model Law does not deal with those issues.

(ii) Certification service providers

53. To associate a key pair with a prospective signatory, a certification service provider (or certification authority) issues a certificate, an electronic record which lists a public key together with the name of the certificate subscriber as the "subject" of the certificate, and may confirm that the prospective signatory identified in the certificate holds the corresponding private key. The principal function of a certificate is to bind a public key with a particular signatory. A "recipient" of the certificate desiring to rely upon a digital signature created by the signatory named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, a level of assurance is provided technically that the digital signature was created by the signatory, and that the portion of the message used in the hash function (and, consequently, the corresponding data message) has not been modified since it was digitally signed."

54. To assure the authenticity of the certificate with respect to both its contents and its source, the certification service provider digitally signs it. The issuing certification service provider's digital signature on the certificate can be verified by using the public key of the certification service provider listed in another certificate by another certification service provider (which may but need not be on a higher level in a

hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. In each case, the issuing certification service provider must digitally sign its own certificate during the operational period of the other certificate used to verify the certification service provider's digital signature. Under the laws of some States, a way of building trust in the digital signature of the certification service provider might be to publish the public key of the certification service provider in an official bulletin (see A/CN.9/484, para. 41).

55. A digital signature corresponding to a message, whether created by the signatory to authenticate a message or by a certification service provider to authenticate its certificate, should generally be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the "operational period" stated in the certificate, which is a condition of the verifiability of a digital signature.

56. To make a public key and its correspondence to a specific signatory readily available for verification, the certificate may be published in a repository or made available by other means. Typically, repositories are on-line databases of certificates and other information available for retrieval and use in verifying digital signatures.

57. Once issued, a certificate may prove to be unreliable, for example in situations where the signatory misrepresents its identity to the certification service provider. In other circumstances, a certificate may be reliable enough when issued but it may become unreliable sometime thereafter. If the private key is "compromised", for example through loss of control of the private key by the signatory, the certificate may lose its trustworthiness or become unreliable, and the certification service provider (at the signatory's request or even without the signatory's consent, depending on the circumstances) may suspend (temporarily interrupt the operational period) or revoke (permanently invalidate) the certificate. Immediately upon suspending or revoking a certificate, the certification service provider may be expected to publish notice of the revocation or suspension or notify persons who enquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

58. Certification authorities could be operated by Government authorities or by private sector service providers. In a number of countries, it is envisaged that, for public policy reasons, only Government entities should be authorized to operate as certification authorities. In other countries, it is considered that certification services should be open to competition from the private sector. Irrespective of whether certification authorities are operated by public entities or by private sector service providers, and of whether certification authorities would need to obtain a license to operate, there is typically more than one certification service provider operating within the PKI. Of particular concern is the relationship between the various certification authorities. Certification authorities within a PKI can be established in a hierarchical structure, where some certification authorities only certify other certification authorities, which provide services directly to users. In such a structure, certification authorities are subordinate to other certification authorities. In other conceivable structures, all certification authorities may operate on an equal footing. In any large PKI, there would likely be both subordinate and superior certification authorities. In any event, in the absence of an international PKI, a number of concerns may arise with respect to the recognition of certificates by certification authorities in foreign countries. The recognition of foreign certificates is often achieved by a method called "cross certification". In such a case, it is necessary that substantially equivalent certification authorities (or certification authorities willing to assume certain risks with regard to the certificates issued by other certification authorities) recognize the services provided by each other, so their respective users can communicate with each other more efficiently and with greater confidence in the trustworthiness of the certificates being issued.

59. Legal issues may arise with regard to cross-certifying or chaining of certificates when there are multiple security policies involved. Examples of such issues may include determining whose misconduct caused a loss, and upon whose representations the user relied. It should be noted that legal rules considered for adoption in certain countries provide that, where the levels of security and policies are made known to the users, and there is no negligence on the part of certification authorities, there should be no liability.

60. It may be incumbent upon the certification service provider or the root authority to ensure that its policy requirements are met on an ongoing basis. While the selection of certification authorities may be based on a number of factors, including the strength of the public key being used and the identity of the user, the trustworthiness of any certification service provider may also depend on its enforcement of certificate-issuing standards and the reliability of its evaluation of data received from users who request certificates. Of particular importance is the liability regime applying to any certification service provider with respect to its compliance with the policy and security requirements of the root authority or superior certification service provider, or with any other applicable requirement, on an ongoing basis. Of equal importance is the obligation of the certification service provider to act in accordance with the representations made by it with respect to its policies and practices, as envisaged in article 9(1)(a) of the new Model Law (see A/CN.9/484, para. 43).

61. In the preparation of the Model Law, the following elements were considered as possible factors to be taken into account when assessing the trustworthiness of a certification service provider: (1) independence (i.e., absence of financial or other interest in underlying transactions); (2) financial resources and financial ability to bear the risk of being held liable for loss; (3) expertise in public-key technology and familiarity with proper security procedures; (4) longevity (certification authorities may be required to produce evidence of certification or decryption keys many years after the underlying transaction has been completed, in the context of a lawsuit or property claim); (5) approval of hardware and software; (6) maintenance of an audit trail and audit by an independent entity; (7) existence of a contingency plan (e.g., "disaster recovery" software or key escrow); (8) personnel selection and management; (9) protection arrangements for the certification service provider's own private key; (10) internal security; (11) arrangements for termination of operations, including notice to users; (12) warranties and representations (given or excluded); (13) limitation of liability; (14) insurance; (15) inter-operability with other certification authorities; (16) revocation procedures (in cases where cryptographic keys might be lost or compromised).

(c) Summary of the digital signature process

62. The use of digital signatures usually involves the following processes, performed either by the signatory or by the receiver of the digitally signed message:

(1) The user generates or is given a unique cryptographic key pair;

(2) The signatory prepares a message (for example, in the form of an electronic mail message) on a computer;

(3) The signatory prepares a "message digest", using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key;

(4) The signatory encrypts the message digest with the private key. The

private key is applied to the message digest text using a mathematical algorithm. The digital signature consists of the encrypted message digest;

(5) The signatory typically attaches or appends its digital signature to the message;

(6) The signatory sends the digital signature and the (unencrypted or encrypted) message to the relying party electronically;

(7) The relying party uses the signatory's public key to verify the signatory's digital signature. Verification using the signatory's public key provides a level of technical assurance that the message came exclusively from the signatory;

(8) The relying party also creates a "message digest" of the message, using the same secure hash algorithm;

(9) The relying party compares the two message digests. If they are the same, then the relying party knows that the message has not been altered after it was signed. Even if one bit in the message has been altered after the message has been digitally signed, the message digest created by the relying party will be different from the message digest created by the signatory;

(10) Where the certification process is resorted to, the relying party obtains a certificate from the certification service provider (including through the signatory or otherwise), which confirms the digital signature on the signatory's message (see A/CN.9/484, para. 44). The certificate contains the public key and name of the signatory (and possibly additional information), digitally signed by the certification service provider.

IV. MAIN FEATURES OF THE MODEL LAW

A. Legislative nature of the Model Law

63. The new Model Law was prepared on the assumption that it should be directly derived from article 7 of the UNCITRAL Model Law on Electronic Commerce and should be considered as a way to provide detailed information as to the concept of a reliable "method used to identify" a person and "to indicate that person's approval" of the information contained in a data message (see A/CN.9/WG.IV/WP.71, para. 49).

64. The question of what form the instrument might take was raised and the importance of considering the relationship of the form to the content was noted. Different approaches were suggested as to what the form might be, which included contractual rules, legislative provisions, or guidelines for States considering enacting legislation on electronic signatures. It was agreed as a working assumption that the text should be prepared as a set of legislative rules with commentary, and not merely as guidelines (see A/CN.9/437, para. 27; A/CN.9/446, para. 25; and A/CN.9/457, paras. 51 and 72). The text was finally adopted as a Model Law (A/CN.9/483, paras. 137-138).

B. Relationship with the UNCITRAL Model Law on Electronic Commerce

1. New Model Law as a separate legal instrument

65. The new provisions could have been incorporated in an extended version of the

UNCITRAL Model Law on Electronic Commerce, for example to form a new part III of the UNCITRAL Model Law on Electronic Commerce. With a view to indicating clearly that the new Model Law could be enacted either independently or in combination with the UNCITRAL Model Law on Electronic Commerce, it was eventually decided that the new Model Law should be prepared as a separate legal instrument (see A/CN.9/465, para. 37). That decision results mainly from the fact that, at the time the new Model Law was being finalized, the UNCITRAL Model Law on Electronic Commerce had already been successfully implemented in a number of countries and was being considered for adoption in many other countries. The preparation of an extended version of the UNCITRAL Model Law on Electronic Commerce might have compromised the success of the original version by suggesting a need to improve on that text by way of an update. In addition, preparing a new version of the UNCITRAL Model Law on Electronic Commerce might have introduced confusion in those countries that had recently adopted the UNCITRAL Model Law on Electronic Commerce.

2. New Model Law fully consistent with the UNCITRAL Model Law on Electronic Commerce

66. In drafting the new Model Law, every effort was made to ensure consistency with both the substance and the terminology of the UNCITRAL Model Law on Electronic Commerce (A/CN.9/465, para. 37). The general provisions of the UNCITRAL Model Law on Electronic Commerce have been reproduced in the new instrument. These are articles 1 (Sphere of application), 2(a),(c) and (d) (Definitions of "data message", "originator" and "addressee"), 3 (Interpretation), 4 (Variation by agreement) and 7 (Signature) of the UNCITRAL Model Law on Electronic Commerce.

67. Based on the UNCITRAL Model Law on Electronic Commerce, the new Model Law is intended to reflect in particular: the principle of media-neutrality; an approach under which functional equivalents of traditional paper-based concepts and practices should not be discriminated against; and extensive reliance on party autonomy (A/CN.9/WG.IV/WP.84, para. 16). It is intended for use both as minimum standards in an "open" environment (i.e., where parties communicate electronically without prior agreement) and, where appropriate, as model contractual provisions or default rules in a "closed" environment (i.e., where parties are bound by pre-existing contractual rules and procedures to be followed in communicating by electronic means).

3. Relationship with article 7 of the UNCITRAL Model Law on Electronic Commerce

68. In the preparation of the new Model Law, the view was expressed that the reference to article 7 of the UNCITRAL Model Law on Electronic Commerce in the text of article 6 of the new Model Law was to be interpreted as limiting the scope of the new Model Law to situations where an electronic signature was used to meet a mandatory requirement of law that certain documents had to be signed for *validity* purposes. Under that view, since the law of most nations contained very few such requirements with respect to documents used for commercial transactions, the scope of the new Model Law was very narrow. It was generally agreed, in response, that such interpretation of article 6 (and of article 7 of the UNCITRAL Model Law on Electronic Commerce) was inconsistent with the interpretation of the words "the law" adopted by the Commission in paragraph 68 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, under which "the words 'the law' are to be understood as encompassing not only statutory or regulatory law but also judicially-created law and other procedural law". In fact, the scope of both article 7 of the UNCITRAL Model Law on Electronic Commerce and article 6 of the new Model Law is particularly broad, since most documents used in the context of commercial transactions are likely to be

faced, in practice, with the requirements of the law of evidence regarding proof in writing (A/CN.9/465, para. 67).

C. *"Framework" rules to be supplemented by technical regulations and contract*

69. As a supplement to the UNCITRAL Model Law on Electronic Commerce, the new Model Law is intended to provide essential principles for facilitating the use of electronic signatures. However, as a "framework", the Model Law itself does not set forth all the rules and regulations that may be necessary (in addition to contractual arrangements between users) to implement those techniques in an enacting State. Moreover, as indicated in this Guide, the Model Law is not intended to cover every aspect of the use of electronic signatures. Accordingly, an enacting State may wish to issue regulations to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Model Law. It is recommended that, should it decide to issue such regulation, an enacting State should give particular attention to the need to preserve flexibility in the operation of electronic signature systems by their users. Commercial practice has a long-standing reliance on the voluntary technical standards process. Such technical standards form the bases of product specifications, of engineering and design criteria and of consensus for research and development of future products. To assure the flexibility such commercial practice relies on, to promote open standards with a view to facilitating interoperability, and to support the objective of cross-border recognition (as described in article 12), States may wish to give due regard to the relationship between any specifications incorporated in or authorized by national regulations, and the voluntary technical standards process (see A/CN.9/484, para. 46).

70. It should be noted that the electronic signature techniques considered in the Model Law, beyond raising matters of procedure that may need to be addressed in the implementing technical regulations, may raise certain legal questions, the answers to which will not necessarily be found in the Model Law, but rather in other bodies of law. Such other bodies of law may include, for example, the applicable administrative, contract, tort, criminal and judicial-procedure law, which the Model Law is not intended to deal with.

D. *Added certainty as to the legal effects of electronic signatures*

71. One of the main features of the new Model Law is to add certainty to the operation of the flexible criterion set forth in article 7 of the UNCITRAL Model Law on Electronic Commerce for the recognition of an electronic signature as functionally equivalent to a hand-written signature. Article 7 of the UNCITRAL Model Law on Electronic Commerce reads as follows:

> "(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
>
> *(a)* a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> *(b)* that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
>
> "(2) Paragraph (1) applies whether the requirement therein is in the form of an

obligation or whether the law simply provides consequences for the absence of a signature.

"(3) The provisions of this article do not apply to the following: [...]".

72. Article 7 is based on the recognition of the functions of a signature in a paper-based environment, as described in paragraph 29 above.

73. With a view to ensuring that a message that was required to be authenticated should not be denied legal value for the sole reason that it was not authenticated in a manner peculiar to paper documents, article 7 adopts a comprehensive approach. It establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements that currently present barriers to electronic commerce. Article 7 focuses on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document. Paragraph (1)(a) establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.

74. Paragraph (1)(b) establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph (1)(a). The method used under paragraph (1)(a) should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all the circumstances, including any agreement between the originator and the addressee of the data message.

75. In determining whether the method used under paragraph (1) is appropriate, legal, technical and commercial factors that may be taken into account include the following: (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4) the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, paras. 53 and 56 to 58).

76. Building on the flexible criterion expressed in article 7(1)(b) of the UNCITRAL Model Law on Electronic Commerce, articles 6 and 7 of the new Model Law establish a mechanism through which electronic signatures that meet objective criteria of technical reliability can be made to benefit from early determination as to their legal effectiveness. Depending on the time at which certainty is achieved as to the recognition of an electronic signature as functionally equivalent to a hand-written signature, the Model Law establishes two distinct regimes. The first and broader regime is that described in article 7 of the UNCITRAL Model Law on Electronic Commerce. It recognizes any "method" that may be used to fulfil a legal requirement for a hand-written signature. The legal effectiveness of such a "method" as an equivalent of a hand-written signature depends upon demonstration of its "reliability" to a trier of fact. The second and narrower regime is that created by the new Model Law. It contemplates

methods of electronic signature that may be recognized by a State authority, a private accredited entity, or the parties themselves, as meeting the criteria of technical reliability set forth in the Model Law (see A/CN.9/484, para. 49). The advantage of such recognition is that it brings certainty to the users of such electronic signature techniques before they actually use the electronic signature technique.

E. Basic rules of conduct for the parties involved

77. The Model Law does not deal in any detail with the issues of liability that may affect the various parties involved in the operation of electronic signature systems. Those issues are left to applicable law outside the Model Law. However, the Model Law sets out criteria against which to assess the conduct of those parties, i.e., the signatory, the relying party and the certification service provider.

78. As to the signatory, the Model Law elaborates on the basic principle that the signatory should apply reasonable care with respect to its electronic signature creation data. The signatory is expected to exercise reasonable care to avoid unauthorized use of that signature creation data. The digital signature in itself does not guarantee that the person who has in fact signed is the signatory. At best, the digital signature provides assurance that it is attributable to the signatory (see A/CN.9/484, para. 50). Where the signatory knows or should have known that the signature creation data has been compromised, the signatory should give notice without undue delay to any person who may reasonably be expected to rely on, or to provide services in support of, the electronic signature. Where a certificate is used to support the electronic signature, the signatory is expected to exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory in connection with the certificate.

79. A relying party is expected to take reasonable steps to verify the reliability of an electronic signature. Where the electronic signature is supported by a certificate, the relying party should take reasonable steps to verify the validity, suspension or revocation of the certificate, and observe any limitation with respect to the certificate.

80. The general duty of a certification service provider is to utilize trustworthy systems, procedures and human resources, and to act in accordance with representations that the supplier makes with respect to its policies and practices. In addition, the certification service provider is expected to exercise reasonable care to ensure the accuracy and completeness of all material representations it makes in connection with a certificate. In the certificate, the supplier should provide essential information allowing the relying party to identify the supplier. It should also represent that: (1) the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued; and (2) the signature creation data was operational on or before the date when the certificate was issued. For the benefit of the relying party, the certification service provider should provide additional information as to: (1) the method used to identify the signatory; (2) any limitation on the purpose or value for which the signature creation data or the certificate may be used; (3) the operational condition of the signature creation data; (4) any limitation on the scope or extent of liability of the certification service provider; (5) whether means exist for the signatory to give notice that a signature creation data has been compromised; and (6) whether a timely revocation service is offered.

81. For the assessment of the trustworthiness of the systems, procedures and human resources utilized by the certification service provider, the Model Law provides an open-ended list of indicative factors.

F. A technology-neutral framework

82. Given the pace of technological innovation, the Model Law provides criteria for the legal recognition of electronic signatures irrespective of the technology used (e.g., digital signatures relying on asymmetric cryptography; biometric devices (enabling the identification of individuals by their physical characteristics, whether by hand or face geometry, fingerprint reading, voice recognition or retina scan, etc.); symmetric cryptography, the use of personal identification numbers (PINs); the use of "tokens" as a way of authenticating data messages through a smart card or other device held by the signatory; digitized versions of hand-written signatures; signature dynamics; and other methods, such as clicking an "OK-box"). The various techniques listed could be used in combination to reduce systemic risk (see A/CN.9/484, para. 52).

G. Non-discrimination of foreign electronic signatures

83. The Model Law establishes as a basic principle that the place of origin, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective in an enacting State (see A/CN.9/484, para. 53). Determination of whether, or the extent to which, a certificate or an electronic signature is capable of being legally effective should not depend on the place where the certificate or the electronic signature was issued (see A/CN.9/483, para. 27) but on its technical reliability). That basic principle is elaborated upon in article 12 (see below, paras. 152-160).

V. ASSISTANCE FROM THE UNCITRAL SECRETARIAT

A. Assistance in drafting legislation

84. In the context of its training and assistance activities, the UNCITRAL secretariat assists States with technical consultations for the preparation of legislation based on the UNCITRAL Model Law on Electronic Signatures. The same assistance is brought to Governments considering legislation based on other UNCITRAL model laws (i.e., the UNCITRAL Model Law on International Commercial Arbitration, the UNCITRAL Model Law on International Credit Transfers, the UNCITRAL Model Law on Procurement of Goods, Construction and Services, the UNCITRAL Model Law on Electronic Commerce, and the UNCITRAL Model Law on Cross-Border Insolvency), or considering adhesion to one of the international trade law conventions prepared by UNCITRAL.

85. Further information concerning the Model Law and other model laws and conventions developed by UNCITRAL, may be obtained from the secretariat at the address below:

International Trade Law Branch, Office of Legal Affairs
United Nations
Vienna International Centre
P.O. Box 500
A-1400, Vienna, Austria

Telephone:	(+43-1) 26060-4060 or 4061
Telecopy:	(+43-1) 26060-5813
Electronic mail:	uncitral@uncitral.org
Internet Home Page:	http://www.uncitral.org

B. Information on the interpretation of legislation based on the Model Law

86. The secretariat welcomes comments concerning the Model Law and the Guide, as well as information concerning enactment of legislation based on the Model Law. Once enacted, the Model Law will be included in the CLOUT information system, which is used for collecting and disseminating information on case law relating to the conventions and model laws that have emanated from the work of UNCITRAL. The purpose of the system is to promote international awareness of the legislative texts formulated by UNCITRAL and to facilitate their uniform interpretation and application. The secretariat publishes, in the six official languages of the United Nations, abstracts of decisions and makes available, against reimbursement of copying expenses, the decisions on the basis of which the abstracts were prepared. The system is explained in a user's guide that is available from the secretariat in hard copy (A/CN.9/SER.C/GUIDE/1) and on the above-mentioned Internet home page of UNCITRAL.

Chapter II. Article-by-article remarks

Title

"Model Law"

87. Throughout its preparation, the instrument has been conceived of as an addition to the UNCITRAL Model Law on Electronic Commerce, which should be dealt with on an equal footing and share the legal nature of its forerunner.

Article 1. Sphere of application

This Law applies where electronic signatures are used in the context* of commercial** activities. It does not override any rule of law intended for the protection of consumers.

*The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies where electronic signatures are used, except in the following situations: [...]."

**The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

General remarks

88. The purpose of article 1 is to delineate the scope of application of the Model Law. The approach used in the Model Law is to provide in principle for the coverage of all factual situations where electronic signatures are used, irrespective of the specific electronic signature or authentication technique being applied. It was felt during the preparation of the Model Law that exclusion of any form or medium by way of a limitation in the scope of the Model Law might result in practical difficulties and would run counter to the purpose of providing truly "media-neutral" as well as "technology-neutral" rules. In the preparation of the Model Law, the principle of technology neutrality was observed by the UNCITRAL Working Group on Electronic Commerce, although it was aware that "digital signatures", i.e., those electronic signatures obtained through the application of dual-key cryptography, were a particularly widespread technology (see A/CN.9/484, para. 54).

Footnote **

89. It was felt that the Model Law should contain an indication that its focus was on the types of situations encountered in the commercial area and that it had been prepared against the background of relationships in trade and finance. For that reason, article 1 refers to "commercial activities" and provides, in footnote **, indications as to what is meant thereby. Such indications, which may be particularly useful for those countries where there does not exist a discrete body of commercial law, are modelled, for reasons of consistency, on the footnote to article 1 of the UNCITRAL Model Law on International Commercial Arbitration (also reproduced as footnote **** to article 1 of the UNCITRAL Model Law on Electronic Commerce). In certain countries, the use of footnotes in a statutory text would not be regarded as acceptable legislative practice. National authorities enacting the Model Law might thus consider the possible inclusion of the text of footnotes in the body of the text itself.

Footnote *

90. The Model Law applies to all kinds of data messages to which a legally significant electronic signature is attached, and nothing in the Model Law should prevent an enacting State from extending the scope of the Model Law to cover uses of electronic signatures outside the commercial sphere. For example, while the focus of the Model Law is not on the relationships between users of electronic signatures and public authorities, the Model Law is not intended to be inapplicable to such relationships. Footnote * provides for alternative wordings, for possible use by enacting States that would consider it appropriate to extend the scope of the Model Law beyond the commercial sphere.

Consumer protection

91. Some countries have special consumer protection laws that may govern certain aspects of the use of information systems. With respect to such consumer legislation, as was the case with previous UNCITRAL instruments (e.g., the UNCITRAL Model Law on International Credit Transfers and the UNCITRAL Model Law on Electronic Commerce), it was felt that an indication should be given that the Model Law had been drafted without special attention being given to issues that might arise in the context of consumer protection. At the same time, it was felt that there was no reason why situations involving consumers should be excluded from the scope of the Model Law by way of a general provision, particularly since the provisions of the Model Law might be found very beneficial for consumer protection, depending on legislation in each enacting State. Article 1 thus recognizes

that any such consumer protection law may take precedence over the provisions in the Model Law. Should legislators come to different conclusions as to the beneficial effect of the Model Law on consumer transactions in a given country, they might consider excluding consumers from the sphere of application of the piece of legislation enacting the Model Law. The question of which individuals or corporate bodies would be regarded as "consumers" is left to applicable law outside the Model Law.

Use of electronic signatures in international and domestic transactions

92. It is recommended that application of the Model Law be made as wide as possible. Particular caution should be used in excluding the application of the Model Law by way of a limitation of its scope to international uses of electronic signatures, since such a limitation may be seen as not fully achieving the objectives of the Model Law. Furthermore, the variety of procedures available under the Model Law to limit the use of electronic signatures if necessary (e.g., for purposes of public policy) may make it less necessary to limit the scope of the Model Law. The legal certainty to be provided by the Model Law is necessary for both domestic and international trade. Discrimination between electronic signatures used domestically and electronic signatures used in the context of international trade transactions might result in a duality of regimes governing the use of electronic signatures, thus creating a serious obstacle to the use such techniques (see A/CN.9/484, para. 55).

References to UNCITRAL documents

A/CN.9/484, paras. 54-55;
A/CN.9/WG.IV/WP.88, annex, paras. 87-91;
A/CN.9/467, paras. 22-24;
A/CN.9/WG.IV/WP.84, para. 22;
A/CN.9/465, paras. 36-42;
A/CN.9/WG.IV/WP.82, para. 21;
A/CN.9/457, paras. 53-64.

Article 2. Definitions

For the purposes of this Law:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message;

(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;

(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;

(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.

Definition of "Electronic signature"

Electronic signature as functional equivalent of hand-written signature

93. The notion of "electronic signature" is intended to cover all traditional uses of a hand-written signature for legal effect, the identification of the signatory and the intent to sign being no more than the smallest common denominator to the various approaches to "signature" found in the various legal systems. Those functions of a hand-written signature were already discussed in the context of the preparation of article 7 of the UNCITRAL Model Law on Electronic Commerce. Thus, defining an electronic signature as capable of indicating approval of information amounts primarily to establishing a technical prerequisite for the recognition of a given technology as capable of creating an equivalent to a hand-written signature. The definition does not disregard the fact that technologies commonly referred to as "electronic signatures" could be used for purposes other than creating a legally-significant signature. The definition simply illustrates the focus of the Model Law on the use of electronic signatures as functional equivalents of hand-written signatures (see A/CN.9/483, para. 62).

Possible other uses of an electronic signature

94. A distinction should be drawn between the legal notion of "signature" and the technical notion of "electronic signature", a term of art which covers practices that do not necessarily involve the production of legally significant signatures. In the preparation of the Model Law, it was felt that the attention of users should be brought to the risk of confusion that might result from the use of the same technical tool for the production of a legally meaningful signature and for other authentication or identification functions (ibid.).

Definition of "Certificate"

Need for a definition

95. The term "certificate", as used in the context of certain types of electronic signatures and as defined in the Model Law, differs little from its general meaning of a document by which a person would confirm certain facts. The only difference is that the certificate is in electronic rather than paper form (see A/CN.9/484, para. 56). However, since the general notion of "certificate" does not exist in all legal systems or indeed in all languages, it was felt useful to include a definition in the context of the Model Law (see A/CN.9/483, para. 65).

Purpose of a certificate

96. The purpose of the certificate is to recognize, show or confirm a link between signature creation data and the signatory. That link is created when the signature creation data is generated (ibid., para. 67).

"signature creation data"

97. In the context of electronic signatures which are not digital signatures, the term 'signature creation data' is intended to designate those secret keys, codes or other elements that, in the process of creating an electronic signature, are used to provide a secure link between the resulting electronic signature and the person of the signatory (see A/CN.9/484, para. 57). For example, in the context of electronic signatures based on biometric devices, the essential element would be the biometric indicator, such as a fingerprint or retina-scan data. The description covers only those core elements that should be kept confidential to ensure the quality of the signature process, to the exclusion of any other element which, although it might contribute to the signature process, could be disclosed without jeopardizing the reliability of the resulting electronic signature. On the other hand, in the context of digital signatures relying on asymmetric cryptography, the core operative element that could be described as "linked to the signatory" is the cryptographic key pair. In the case of digital signatures, both the public and the private key are linked to the person of the signatory. Since the prime purpose of a certificate, in the context of digital signatures, is to confirm the link between the public key and the signatory (see paras. 53-56 and 62 (10) above), it is also necessary that the public key must be certified as belonging to the signatory. While only the private key is covered by this description of "signature creation data", it is important to state, for the avoidance of doubt, that in the context of digital signatures the definition of "certificate" in article 2 (b) should be taken to include the confirming of the link between the signatory and the signatory's public key. Also among the elements not to be covered by this description is the text being electronically signed, although it also plays an important role in the signature-creation process (through a hash function or otherwise). Article 6 expresses the idea that the signature creation data should be linked to the signatory and to no other person (A/CN.9/483, para. 75)".

Definition of "Data message"

98. The definition of "data message" is taken from article 2 of the UNCITRAL Model Law on Electronic Commerce as a broad notion encompassing all messages generated in the context of electronic commerce, including web-based commerce (ibid., para. 69). The notion of "data message" is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of "message" includes the notion of "record".

99. The reference to "similar means" is intended to reflect the fact that the Model Law was not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments. The aim of the definition of "data message" is to encompass all types of messages that are generated, stored, or communicated in essentially paperless form. For that purpose, all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means listed in the definition are intended to be covered by the reference to "similar means", although, for example, "electronic" and "optical" means of communication might not be, strictly speaking, similar. For the purposes of the Model Law, the word "similar" connotes "functionally equivalent".

100. The definition of "data message" is also intended to apply in case of revocation or amendment. A data message is presumed to have a fixed information content but it may be revoked or amended by another data message (Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, paras. 30-32).

Definition of "Signatory"

"a person"

101. Consistent with the approach taken in the UNCITRAL Model Law on Electronic Commerce, any reference in the new Model Law to a "person" should be understood as covering all types of persons or entities, whether physical, corporate or other legal persons (A/CN.9/483, para. 86).

"on behalf of the person it represents"

102. The analogy to hand-written signatures may not always be suitable for taking advantage of the possibilities offered by modern technology. In a paper-based environment, for instance, legal entities cannot strictly speaking be signatories of documents drawn up on their behalf, because only natural persons can produce authentic hand-written signatures. Electronic signatures, however, can be conceived so as to be attributable to companies, or other legal entities (including governmental and other public authorities), and there may be situations where the identity of the person who actually generates the signature, where human action is required, is not relevant for the purposes for which the signature was created (ibid., para. 85).

103. Nevertheless, under the Model Law, the notion of "signatory" cannot be severed from the person or entity that actually generated the electronic signature, since a number of specific obligations of the signatory under the Model Law are logically linked to actual control over the signature creation data. However, in order to cover situations where the signatory would be acting in representation of another person, the phrase "or on behalf of the person it represents" has been retained in the definition of "signatory". The extent to which a person would be bound by an electronic signature generated "on its behalf" is a matter to be settled in accordance with the law governing, as appropriate, the legal relationship between the signatory and the person on whose behalf the electronic signature is generated, on the one hand, and the relying party, on the other hand. That matter, as well as other matters pertaining to the underlying transaction, including issues of agency and other questions as to who bears the ultimate liability for failure by the signatory to comply with its obligations under article 8 (whether the signatory or the person represented by the signatory) are outside the scope of the Model Law (ibid., paras. 86-87).

Definition of "Certification service provider"

104. As a minimum, the certification service provider as defined for the purposes of the Model Law would have to provide certification services, possibly together with other services (ibid., para. 100).

105. No distinction has been drawn in the Model Law between situations where a certification service provider engages in the provision of certification services as its main activity or as an ancillary business, on a habitual or an occasional basis, directly or through a subcontractor. The definition covers all entities that provide certification services within the scope of the Model Law, i.e., "in the context of commercial activities". However, in view of that limitation in the scope of application of the Model Law, entities that issued certificates for internal purposes and not for commercial purposes would not fall under the category "certification service providers" as defined in article 2 (ibid., paras. 94-99).

Definition of 'Relying party"

106. The definition of "relying party" is intended to ensure symmetry in the

definition of the various parties involved in the operation of electronic signature schemes under the Model Law (ibid., para. 107). For the purposes of that definition, "act" should be interpreted broadly to cover not only a positive action but also an omission (ibid., para. 108).

References to UNCITRAL documents

A/CN.9/484, paras. 56-57;
A/CN.9/WG.IV/WP.88, annex, paras. 92-105;
A/CN.9/483, paras. 59-109;
A/CN.9/WG.IV/WP.84, paras. 23-36;
A/CN.9/465, para. 42;
A/CN.9/WG.IV/WP.82, paras. 22-33;
A/CN.9/457, paras. 22-47; 66-67; 89; 109;
A/CN.9/WG.IV/WP.80, paras. 7-10;
A/CN.9/WG.IV/WP.79, para. 21;
A/CN.9/454, para. 20;
A/CN.9/WG.IV/WP.76, paras. 16-20;
A/CN.9/446, paras. 27-46 (draft article 1), 62-70 (draft article 4), 113-131 (draft article 8), 132-133 (draft article 9);
A/CN.9/WG.IV/WP.73, paras. 16-27, 37-38, 50-57, and 58-60;
A/CN.9/437, paras. 29-50 and 90-113 (draft articles A, B and C); and
A/CN.9/WG.IV/WP.71, paras. 52-60.

Article 3. Equal treatment of signature technologies

Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 (1) or otherwise meets the requirements of applicable law.

Neutrality as to technology

107. Article 3 embodies the fundamental principle that no method of electronic signature should be discriminated against, i.e., that all technologies would be given the same opportunity to satisfy the requirements of article 6. As a result, there should be no disparity of treatment between electronically-signed messages and paper documents bearing hand-written signatures, or between various types of electronically-signed messages, provided that they meet the basic requirements set forth in article 6(1) of the Model Law or any other requirement set forth in applicable law. Such requirements might, for example, prescribe the use of a specifically designated signature technique in certain identified situations, or might otherwise set a standard that might be higher or lower than that set forth in article 7 of the UNCITRAL Model Law on Electronic Commerce (and article 6 of the Model Law). The fundamental principle of non-discrimination is intended to find general application. It should be noted, however, that such a principle is not intended to affect the freedom of contract recognized under article 5. As between themselves and to the extent permitted by law, the parties should thus remain free to exclude by agreement the use of certain electronic signature techniques. By stating that "nothing in this Law shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature", article 3 merely indicates that the form in which a certain electronic signature is applied cannot be used as the only reason for which that signature would be denied legal effectiveness. However,

article 3 should not be misinterpreted as establishing the legal validity of any given signature technique or of any electronically-signed information.

References to UNCITRAL documents

A/CN.9/WG.IV/WP.88, annex, para. 106;
A/CN.9/467, paras. 25-32;
A/CN.9/WG.IV/WP.84, para. 37;
A/CN.9/465, paras. 43-48;
A/CN.9/WG.IV/WP.82, para. 34;
A/CN.9/457, paras. 53-64.

Article 4. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Source

108. Article 4 is inspired by article 7 of the United Nations Convention on Contracts for the International Sale of Goods, and reproduced from article 3 of the UNCITRAL Model Law on Electronic Commerce. It is intended to provide guidance for interpretation of the Model Law by arbitral tribunals, courts and national or local administrative authorities. The expected effect of article 4 is to limit the extent to which a uniform text, once incorporated in local legislation, would be interpreted only by reference to the concepts of local law.

Paragraph (1)

109. The purpose of paragraph (1) is to draw the attention of any person who might be called upon to apply the Model Law to the fact that the provisions of the Model Law (or the provisions of the instrument implementing the Model Law), while enacted as part of domestic legislation and therefore domestic in character, should be interpreted with reference to its international origin in order to ensure uniformity in the interpretation of the Model Law in all enacting countries.

Paragraph (2)

110. Amongst the general principles on which the Model Law is based, the following non-exhaustive list may be found applicable: (1) to facilitate electronic commerce among and within nations; (2) to validate transactions entered into by means of new information technologies; (3) to promote and encourage in a technology-neutral way the implementation of new information technologies in general and electronic signatures in particular; (4) to promote the uniformity of law; and (5) to support commercial practice. While the general purpose of the Model Law is to facilitate the use of electronic signatures, it should not be construed in any way as imposing their use.

References to UNCITRAL documents

A/CN.9/WG.IV/WP.88, annex, paras. 107-109;
A/CN.9/467, paras. 33-35;
A/CN.9/WG.IV/WP.84, para. 38.
A/CN.9/465, paras. 49-50;
A/CN.9/WG.IV/WP.82, para. 35.

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.

Deference to applicable law

111. The decision to undertake the preparation of the Model Law was based on the recognition that, in practice, solutions to the legal difficulties raised by the use of modern means of communication are mostly sought within contracts. The Model Law is thus intended to support the principle of party autonomy. However, applicable law may set limits to the application of that principle. Article 5 should not be misinterpreted as allowing the parties to derogate from mandatory rules, e.g., rules adopted for reasons of public policy. Neither should article 5 be misinterpreted as encouraging States to establish mandatory legislation limiting the effect of party autonomy with respect to electronic signatures or otherwise inviting States to restrict the freedom of parties to agree as between themselves on issues of form requirements governing their communications.

112. The principle of party autonomy applies broadly with respect to the provisions of the Model Law, since the Model Law does not contain any mandatory provision. That principle also applies in the context of article 13(1). Therefore, although the courts of the enacting State or authorities responsible for the application of the Model Law should not deny or nullify the legal effects of a foreign certificate only on the basis of the place where the certificate is issued, article 13(1) does not limit the freedom of the parties to a commercial transaction to agree on the use of certificates that originate from a particular place (A/CN.9/483, para. 112).

Expressed or implied agreement

113. As to the way in which the principle of party autonomy is expressed in article 5, it was generally admitted in the preparation of the Model Law that variation by agreement might be expressed or implied. The wording of article 5 has been kept in line with article 6 of the United Nations Convention on Contracts for the International Sale of Goods (A/CN.9/467, para. 38).

Bilateral or multilateral agreement

114. Article 5 is intended to apply not only in the context of relationships between originators and addressees of data messages but also in the context of relationships involving intermediaries. Thus, the provisions of the Model Law could be varied either by bilateral or multilateral agreements between the parties, or by system rules agreed to by the parties. Typically, applicable law would limit party autonomy to rights and obligations arising as between parties so as to avoid any implication as to the rights and obligations of third parties.

References to UNCITRAL documents

A/CN.9/WG.IV/WP.88, annex, paras. 110-113;
A/CN.9/467, paras. 36-43;
A/CN.9/WG.IV/WP.84, paras. 39-40;
A/CN.9/465, paras. 51-61;
A/CN.9/WG.IV/WP.82, paras. 36-40;
A/CN.9/457, paras. 53-64.

Article 6. Compliance with a requirement for a signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) the signature creation data are, at the time of signing, under the control of the signatory and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Paragraph (3) does not limit the ability of any person:

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

(5) The provisions of this article do not apply to the following: [...]

Importance of article 6

115. Article 6 is one of the core provisions of the Model Law. Article 6 is intended to build upon article 7 of the UNCITRAL Model Law on Electronic Commerce and to provide guidance as to how the test of reliability in article 7(1)(b)

can be satisfied. In interpreting article 6, it should be borne in mind that the purpose of that provision is to ensure that, where any legal consequence would have flowed from the use of a hand-written signature, the same consequence should flow from the use of a reliable electronic signature.

Paragraphs (1), (2) and (5)

116. Paragraphs (1), (2), and (5) of article 6 introduce provisions drawn from article 7(1)(b), (2), and (3) of the UNCITRAL Model Law on Electronic Commerce, respectively. Wording inspired by article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce is already included in the definition of "electronic signature" under article 2(a).

Notions of "identity" and "identification"

117. The Working Group agreed that, for the purpose of defining "electronic signature" under the Model Law, the term "identification" could be broader than mere identification of the signatory by name. The concept of identity or identification includes distinguishing him or her, by name or otherwise, from any other person, and may refer to other significant characteristics, such as position or authority, either in combination with a name or without reference to the name. On that basis, it is not necessary to distinguish between identity and other significant characteristics, nor to limit the Model Law to those situations in which only identity certificates which name the signatory are used (A/CN.9/467, paras. 56-58).

Effect of the Model Law varying with level of technical reliability

118. In the preparation of the Model Law, the view was expressed that (either through a reference to the notion of "enhanced electronic signature" or through a direct mention of criteria for establishing the technical reliability of a given signature technique) a dual purpose of article 6 should be to establish: (1) that legal effects would result from the application of those electronic signature techniques that were recognized as reliable; and (2), conversely, that no such legal effects would flow from the use of techniques of a lesser reliability. It was generally felt, however, that a more subtle distinction might need to be drawn between the various possible electronic signature techniques, since the Model Law should avoid discriminating against any form of electronic signature, unsophisticated and insecure though it might appear in given circumstances. Therefore, any electronic signature technique applied for the purpose of signing a data message under article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce would be likely to produce legal effects, provided that it was sufficiently reliable in the light of all the circumstances, including any agreement between the parties. However, under article 7 of the UNCITRAL Model Law on Electronic Commerce, the determination of what constitutes a reliable method of signature in the light of the circumstances, can be made only by a court or other trier of fact intervening *ex post*, possibly long after the electronic signature has been used. In contrast, the new Model Law is expected to create a benefit in favour of certain techniques, which are recognized as particularly reliable, irrespective of the circumstances in which they are used. That is the purpose of paragraph (3), which is expected to create certainty (through either a presumption or a substantive rule), at or before the time any such technique of electronic signature is used (*ex ante*), that using a recognized technique will result in legal effects equivalent to those of a hand-written signature. Thus, paragraph (3) is an essential provision if the new Model Law is to meet its goal of providing more certainty than readily offered by the UNCITRAL Model Law on Electronic Commerce as to the legal effect to be expected from the use of particularly reliable types of electronic signatures (see A/CN.9/465, para. 64).

Presumption or substantive rule

119. In order to provide certainty as to the legal effect resulting from the use of an electronic signature as defined under article 2, paragraph (3) expressly establishes the legal effects that would result from the conjunction of certain technical characteristics of an electronic signature (see A/CN.9/484, para. 58). As to how those legal effects would be established, enacting States, depending on their law of civil and commercial procedure, should be free to adopt a presumption or to proceed by way of a direct assertion of the linkage between certain technical characteristics and the legal effect of a signature (see A/CN.9/467, paras. 61-62).

Intent of signatory

120. A question remains as to whether any legal effect should result from the use of electronic signature techniques that may be made with no clear intent by the signatory of becoming legally bound by approval of the information being electronically signed. In any such circumstance, the second function described in article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce is not fulfilled since there is no "intent of indicating any approval of the information contained in the data message". The approach taken in the Model Law is that the legal consequences of the use of a hand-written signature should be replicated in an electronic environment. Thus, by appending a signature (whether hand-written or electronic) to certain information, the signatory should be presumed to have approved the linking of its identity with that information. Whether such a linking should produce legal effects (contractual or other) would result from the nature of the information being signed, and from any other circumstances, to be assessed according to the law applicable outside the Model Law. In that context, the Model Law is not intended to interfere with the general law of contracts or obligations (see A/CN.9/465, para. 65).

Criteria of technical reliability

121. Subparagraphs (a) to (d) of paragraph (3) are intended to express objective criteria of technical reliability of electronic signatures. Subparagraph (a) focuses on the objective characteristics of the signature creation data, which must be "linked to the signatory and to no other person". From a technical point of view, the signature creation data could be uniquely "linked" to the signatory, without being "unique" in itself. The linkage between the data used for creation of the signature and the signatory is the essential element (A/CN.9/467, para. 63). While certain electronic signature creation data may be shared by a variety of users, for example where several employees would share the use of a corporate signature-creation data, that data must be capable of identifying one user unambiguously in the context of each electronic signature.

Sole control of signature creation data by the signatory

122. Subparagraph (b) deals with the circumstances in which the signature creation data is used. At the time it is used, the signature creation data must be under the sole control of the signatory. In relation to the notion of sole control by the signatory, a question is whether the signatory would retain its ability to authorize another person to use the signature creation data on its behalf. Such a situation might arise where the signature creation data is used in the corporate context where the corporate entity would be the signatory but would require a number of persons to be able to sign on its behalf (A/CN.9/467, para. 66). Another example may be found in business applications such as the one where signature creation data exist on a network and are capable of being used by a number of people. In that situation, the network would

presumably relate to a particular entity which would be the signatory and maintain control over the signature creation data. If that was not the case, and the signature creation data was widely available, it should not be covered by the Model Law (A/CN.9/467, para. 67). Where a single key is operated by more than one person in the context of a "split-key" or other "shared-secret" scheme, reference to "the signatory" means a reference to those persons jointly (A/CN.9/483, para. 152).

Agency

123. Subparagraphs (a) and (b) converge to ensure that the signature creation data is capable of being used by only one person at any given time, principally the time of signing, and not by some other person as well (see above, para. 103). The question of agency or authorized use of the signature creation data is addressed in the definition of "signatory" (A/CN.9/467, para. 68).

Integrity

124. Subparagraphs (c) and (d) deal with the issues of integrity of the electronic signature and integrity of the information being signed electronically. It would have been possible to combine the two provisions to emphasize the notion that, where a signature is attached to a document, the integrity of the document and the integrity of the signature are so closely related that it is difficult to conceive of one without the other. However, it was decided that the Model Law should follow the distinction drawn in the UNCITRAL Model Law on Electronic Commerce between articles 7 and 8. Although some technologies provide both authentication (article 7 of the UNCITRAL Model Law on Electronic Commerce) and integrity (article 8 of the UNCITRAL Model Law on Electronic Commerce), those concepts can be seen as distinct legal concepts and treated as such. Since a hand-written signature provides neither a guarantee of the integrity of the document to which it is attached nor a guarantee that any change made to the document would be detectable, the functional equivalence approach requires that those concepts should not be dealt with in a single provision. The purpose of paragraph (3)(c) is to set forth the criterion to be met in order to demonstrate that a particular method of electronic signature is reliable enough to satisfy a requirement of law for a signature. That requirement of law could be met without having to demonstrate the integrity of the entire document (see A/CN.9/467, paras. 72-80).

125. Subparagraph (d) is intended primarily for use in those countries where existing legal rules governing the use of hand-written signatures could not accommodate a distinction between integrity of the signature and integrity of the information being signed. In other countries, subparagraph (d) might create a signature that would be more reliable than a hand-written signature and thus go beyond the concept of functional equivalent to a signature. In certain jurisdictions, the effect of subparagraph (d) may be to create a functional equivalent to an original document (see A/CN.9/484, para. 62).

Electronic signature of portion of a message

126. In subparagraph (d), the necessary linkage between the signature and the information being signed is expressed so as to avoid the implication that the electronic signature could apply only to the full contents of a data message. In fact, the information being signed, in many instances, will be only a portion of the information contained in the data message. For example, an electronic signature may relate only to information appended to the message for transmission purposes.

Variation by agreement

127. Paragraph (3) is not intended to limit the application of article 5 and of any applicable law recognizing the freedom of the parties to stipulate in any relevant agreement that a given signature technique would be treated among themselves as a reliable equivalent of a hand-written signature.

128. Paragraph (4)(a) is intended to provide a legal basis for the commercial practice under which many commercial parties would regulate by contract their relationships regarding the use of electronic signatures (see A/CN.9/484, para. 63).

Possibility to adduce evidence of the non-reliability of an electronic signature

129. Paragraph (4)(b) is intended to make it clear that the Model Law does not limit any possibility that may exist to rebut the presumption contemplated in paragraph (3) (see A/CN.9/484, para. 63).

Exclusions from the scope of article 6

130. The principle embodied in paragraph (5) is that an enacting State may exclude from the application article 6 certain situations to be specified in the legislation enacting the Model Law. An enacting State may wish to exclude specifically certain types of situations, depending in particular on the purpose for which a formal requirement for a hand-written signature has been established. A specific exclusion might be considered, for example, in the context of formalities required pursuant to international treaty obligations of the enacting State and other kinds of situations and areas of law that are beyond the power of the enacting State to change by means of a statute.

131. Paragraph (5) was included with a view to enhancing the acceptability of the Model Law. It recognizes that the matter of specifying exclusions should be left to enacting States, an approach that would take better account of differences in national circumstances. However, it should be noted that the objectives of the Model Law would not be achieved if paragraph (5) were used to establish blanket exceptions, and the opportunity provided by paragraph (5) in that respect should be avoided. Numerous exclusions from the scope of article 6 would raise needless obstacles to the development of electronic signatures, since what the Model Law contains are very fundamental principles and approaches that are expected to find general application (see A/CN.9/484, para. 63).

References to UNCITRAL documents

A/CN.9/484, paras. 58-63;
A/CN.9/WG.IV/WP.88, annex, paras. 114-126;
A/CN.9/467, paras. 44-87;
A/CN.9/WG.IV/WP.84, paras. 41-47;
A/CN.9/465, paras. 62-82;
A/CN.9/WG.IV/WP.82, paras. 42-44;
A/CN.9/457, paras. 48-52;
A/CN.9/WG.IV/WP.80, paras. 11-12.

Article 7. Satisfaction of article 6

(1) *[Any person, organ or authority, whether public or private,*

specified by the enacting State as competent] may determine which electronic signatures satisfy the provisions of article 6.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

(3) Nothing in this article affects the operation of the rules of private international law.

Pre-determination of status of electronic signature

132. Article 7 describes the role played by the enacting State in establishing or recognizing any entity that might validate the use of electronic signatures or otherwise certify their quality. Like article 6, article 7 is based on the idea that what is required to facilitate the development of electronic commerce is certainty and predictability at the time when commercial parties make use of electronic signature techniques, not at the time when there is a dispute before a court. Where a particular signature technique can satisfy requirements for a high degree of reliability and security, there should be a means for assessing the technical aspects of reliability and security and for according the signature technique some form of recognition.

Purpose of article 7

133. The purpose of article 7 is to make it clear that an enacting State may designate an organ or authority that will have the power to make determinations as to what specific technologies may benefit from the rule established under article 6. Article 7 is not an enabling provision that could, or would, necessarily be enacted by States in its present form. However, it is intended to convey a clear message that certainty and predictability can be achieved by determining which electronic signature techniques satisfy the reliability criteria of article 6, provided that such determination is made in accordance with international standards. Article 7 should not be interpreted in a manner that would either prescribe mandatory legal effects for the use of certain types of signature techniques, or would restrict the use of technology to those techniques determined to satisfy the reliability requirements of article 6. Parties should be free, for example, to use techniques that had not been determined to satisfy articles 6, if that was what they had agreed to do. They should also be free to show, before a court or arbitral tribunal, that the method of signature they had chosen to use did satisfy the requirements of article 6, even though not the subject of a prior determination to that effect.

Paragraph (1)

134. Paragraph (1) makes it clear that any entity that might validate the use of electronic signatures or otherwise certify their quality would not have to be established as a State authority. Paragraph (1) should not be read as making a recommendation to States as to the only means of achieving recognition of signature technologies, but rather as indicating the limitations that should apply if States wished to adopt such an approach.

Paragraph (2)

135. With respect to paragraph (2), the notion of "standard" should not be limited to standards developed, for example, by the International Standards Organization (ISO) and the Internet Engineering Task Force (IETF), or to other technical standards. The word "standards" should be interpreted in a broad sense, which

would include industry practices and trade usages, texts emanating from such international organizations as the International Chamber of Commerce, the regional accreditation bodies operating under the aegis of the ISO (see A/CN.9/484, para. 66), the World Wide Web Consortium (W3C), as well as the work of UNCITRAL itself (including this Model Law and the UNCITRAL Model Law on Electronic Commerce). The possible lack of relevant standards should not prevent the competent persons or authorities from making the determination referred to in paragraph (1). As to the reference to "recognized" standards, a question might be raised as to what constitutes "recognition" and of whom such recognition is required (see A/CN.9/465, para. 94). That question is discussed under article 12 (see below, para. 159).

Paragraph (3)

136. Paragraph (3) is intended to make it abundantly clear that the purpose of article 7 is not to interfere with the normal operation of the rules of private international law (see A/CN.9/467, para. 94). In the absence of such a provision, article 7 might be misinterpreted as encouraging enacting States to discriminate against foreign electronic signatures on the basis of non-compliance with the rules set forth by the relevant person or authority under paragraph (1).

References to UNCITRAL documents

A/CN.9/484, paras. 64-66;
A/CN.9/WG.IV/WP.88, paras. 127-131;
A/CN.9/467, paras. 90-95;
A/CN.9/WG.IV/WP.84, para. 49-51;
A/CN.9/465, paras. 90-98;
A/CN.9/WG.IV/WP.82, para. 46;
A/CN.9/457, paras. 48-52;
A/CN.9/WG.IV/WP.80, para. 15.

Article 8. Conduct of the signatory

(1) Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

(a) exercise reasonable care to avoid unauthorized use of its signature creation data;

(b) without undue delay, notify any person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:

(i) the signatory knows that the signature creation data has been compromised; or
(ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or which are to be

included in the certificate.

(2) A signatory shall be liable for its failure to satisfy the requirements of paragraph (1).

Title

137. Article 8 (and articles 9 and 11) had been initially planned to contain rules regarding the obligations and liabilities of the various parties involved (the signatory, the relying party and any certification services provider). However, the rapid changes affecting the technical and commercial aspects of electronic commerce, together with the role currently played by self-regulation in the field of electronic commerce in certain countries, made it difficult to achieve consensus as to the contents of such rules. The articles have been drafted so as to embody a minimal "code of conduct" of the various parties. As indicated in the context of article 9 with respect to certification service providers (see below, para. 144), the Model Law does not require from a signatory a degree of diligence or trustworthiness that bears no reasonable relationship to the purposes for which the electronic signature or certificate is used (see A/CN.9/484, para. 67). The Model Law thus favours a solution which links the obligations set forth in both articles 8 and 9 to the production of legally-significant electronic signatures (A/CN.9/483, para. 117). The principle of the signatory's liability for failure to comply with paragraph (1) is set forth in paragraph (2); the extent of such liability for failure to abide by that code of conduct is left to the law applicable outside the Model Law (see below, para. 141).

Paragraph (1)

138. Subparagraphs (a) and (b) apply generally to all electronic signatures, while subparagraph (c) applies only to those electronic signatures that are supported by a certificate. The obligation in paragraph (1) (a), in particular, to exercise reasonable care to prevent unauthorized use of a signature creation data, constitutes a basic obligation that is, for example, generally contained in agreements concerning the use of credit cards. Under the policy adopted in paragraph (1), such an obligation should also apply to any electronic signature creation data that could be used for the purpose of expressing legally significant intent. However, the provision for variation by agreement in article 5 allows the standards set in article 8 to be varied in areas where they would be thought to be inappropriate, or to lead to unintended consequences.

139. Paragraph (1) (b) refers to the notion of "person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature". Depending on the technology being used, such a "relying party" may be not only a person who might seek to rely on the signature, but also a person such as a certification service provider, a certificate revocation service provider and any other interested party.

140. Paragraph (1) (c) applies where a certificate is used to support the signature creation data. The "life-cycle of the certificate" is intended to be interpreted broadly as covering the period starting with the application for the certificate or the creation of the certificate and ending with the expiry or revocation of the certificate.

Paragraph (2)

141. Paragraph (2) does not specify either the consequences or the limits of liability, both of which are left to national law. However, even though it leaves the consequences of liability up to national law, paragraph (2) serves to give a clear

signal to enacting States that liability should attach to a failure to satisfy the obligations set forth in paragraph (1). Paragraph (2) is based on the conclusion reached by the Working Group at its thirty-fifth session that it might be difficult to achieve consensus as to what consequences might flow from the liability of the signatory. Depending on the context in which the electronic signature is used, such consequences might range, under existing law, from the signatory being bound by the contents of the message to liability for damages. Accordingly, paragraph (2) merely establishes the principle that the signatory should be liable for failure to meet the requirements of paragraph (1), and leaves it to the law applicable outside the Model Law in each enacting State to deal with the legal consequences that would flow from such liability (A/CN.9/465, para. 108).

References to UNCITRAL documents

A/CN.9/484, paras. 67-69;
A/CN.9/WG.IV/WP.88, annex, paras. 132-136;
A/CN.9/467, paras. 96-104;
A/CN.9/WG.IV/WP.84, para. 52-53;
A/CN.9/465, paras. 99-108;
A/CN.9/WG.IV/WP.82, paras. 50-55;
A/CN.9/457, paras. 65-98;
A/CN.9/WG.IV/WP.80, paras. 18-19.

Article 9. Conduct of the certification service provider

(1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

(a) act in accordance with representations made by it with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain from the certificate:

(i) the identity of the certification service provider;
(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
(iii) that the signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means which enable a relying party to ascertain, where relevant, from the certificate or otherwise:

(i) the method used to identify the signatory;
(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
(iii) that the signature creation data are valid and have not

been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signatory to give notice pursuant to article 8 (1) (b);

(vi) whether a timely revocation service is offered;

(e) where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8(1)(b) and, where services under subparagraph d (vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider shall be liable for its failure to satisfy the requirements of paragraph (1).

Paragraph (1)

142. Subparagraph (a) expresses the basic rule that a certification service provider should adhere to the representations and commitments made by that supplier, for example in a certification practices statement or in any other type of policy statement.

143. Subparagraph (c) defines the essential contents and the core effect of any certificate under the Model Law. It is important to note that, in the case of digital signatures, it must also be possible to ascertain the association of the signatory with the public key, as well as with the private key (A/CN.9/484, para. 71). Subparagraph (d) lists additional elements to be included in the certificate or otherwise made available or accessible to the relying party, where they would be relevant to a particular certificate. Subparagraph (e) is not intended to apply to certificates such as transactional certificates, which are one-time certificates, or low-cost certificates for low-risk applications, both of which might not be subject to revocation.

144. It may be thought that the duties and obligations provided in article 9 can reasonably be expected to be complied with by any certification service provider, and not only those who issue "high value" certificates. However, the Model Law does not require from a signatory or a certification service provider a degree of diligence or trustworthiness that bears no reasonable relationship to the purposes for which the electronic signature or certificate is used (see above, para. 137). The Model Law thus favours a solution which links the obligations set forth in both articles 8 and 9 to the production of legally-significant electronic signatures (A/CN.9/483, para. 117). By limiting the scope of article 9 to the broad range of situations where certification services are provided to support an electronic signature that may be used for legal effect as a signature, the Model Law does not intend to create new types of legal effects for signatures (ibid., para. 119).

Paragraph (2)

145. Paragraph (2) leaves it up to national law to determine the consequences of liability (see A/CN.9/484, para. 73). Subject to applicable rules of national law, paragraph (2) is not intended by its authors to be interpreted as a rule of absolute liability. It was not foreseen that the effect of paragraph (2) would be to exclude the possibility for the certification service provider to prove, for example, the absence of

fault or contributory fault.

146. Early drafts of article 9 contained an additional paragraph, which addressed the consequences of liability as set forth in paragraph (2). In the preparation of the Model Law, it was observed that the question of the liability of certification service providers would not be sufficiently addressed by adopting a single provision along the lines of paragraph (2). While paragraph (2) may state an appropriate principle for application to signatories, it may not be sufficient for addressing the professional and commercial activities covered by article 9. One possible way of compensating such insufficiency would have been to list in the text of the Model Law the factors to be taken into account in assessing any loss resulting from failure by the certification service provider to satisfy the requirements of paragraph (1). It was finally decided that a non-exhaustive list of indicative factors should be contained in this Guide. In assessing the liability of the certification service provider, the following factors should be taken into account, *inter alia*: (a) the cost of obtaining the certificate; (b) the nature of the information being certified; (c) the existence and extent of any limitation on the purpose for which the certificate may be used; (d) the existence of any statement limiting the scope or extent of the liability of the certification service provider; and (e) any contributory conduct by the relying party. In the preparation of the Model Law, it was generally agreed that, in determining the recoverable loss in the enacting State, weight should be given to the rules governing limitation of liability in the State where the certification service provider was established or in any other State whose law would be applicable under the relevant conflict-of-laws rule (A/CN.9/484, para. 74).

References to UNCITRAL documents

A/CN.9/484, paras. 70-74;
A/CN.9/WG.IV/WP.88, annex, paras. 137-141;
A/CN.9/483, paras. 114-127;
A/CN.9/467, paras. 105-129;
A/CN.9/WG.IV/WP.84, para. 54-60;
A/CN.9/465, paras. 123-142 (draft article 12);
A/CN.9/WG.IV/WP.82, paras. 59-68 (draft article 12);
A/CN.9/457, paras. 108-119;
A/CN.9/WG.IV/WP.80, paras. 22-24.

Article 10. Trustworthiness

For the purposes of article 9(1)(f), in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

Flexibility of the notion of "trustworthiness"

147. Article 10 was initially drafted as part of article 9. Although that part later became a separate article, it is mainly intended to assist with the interpretation of the notion of "trustworthy systems, procedures and human resources" in article 9(1)(f). Article 10 is set forth as a non-exhaustive list of factors to be taken into account in determining trustworthiness. That list is intended to provide a flexible notion of trustworthiness, which could vary in content depending upon what is expected of the certificate in the context in which it is created.

References to UNCITRAL documents

A/CN.9/WG.IV/WP.88, annex, para. 142;
A/CN.9/483, paras. 128-133;
A/CN.9/467, paras. 114-119.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and

(ii) observe any limitation with respect to the certificate.

Reasonableness of reliance

148. Article 11 reflects the idea that a party who intends to rely on an electronic signature should bear in mind the question whether and to what extent such reliance is reasonable in the light of the circumstances. It is not intended to deal with the issue of the validity of an electronic signature, which is addressed under article 6 and should not depend upon the conduct of the relying party. The issue of the validity of an electronic signature should be kept separate from the issue of whether it is reasonable for a relying party to rely on a signature that does not meet the standard set forth in article 6.

Consumer issues

149. While article 11 might place a burden on relying parties, particularly where

such parties are consumers, it may be recalled that the Model Law is not intended to overrule any rule governing the protection of consumers. However, the Model Law might play a useful role in educating all the parties involved, including relying parties, as to the standard of reasonable conduct to be met with respect to electronic signatures. In addition, establishing a standard of conduct under which the relying party should verify the reliability of the signature through readily accessible means may be seen as essential to the development of any public-key infrastructure system.

Notion of "relying party"

150. Consistent with its definition, the notion of "relying party" is intended to cover any party that might rely on an electronic signature. Depending on the circumstances, a "relying party" might thus be any person having or not a contractual relationship with the signatory or the certification services provider. It is even conceivable that the certification services provider or the signatory might itself become a "relying party". However, that broad notion of "relying party" should not result in the subscriber of a certificate being placed under an obligation to verify the validity of the certificate it purchases from the certification services provider.

Failure to comply with requirements of article 11

151. As to the possible impact of establishing as a general obligation that the relying party should verify the validity of the electronic signature or certificate, a question arises where the relying party fails to comply with the requirements of article 11. Should it fail to comply with those requirements, the relying party should not be precluded from availing itself of the signature or certificate if reasonable verification would not have revealed that the signature or certificate was invalid. The requirements of article 11 are not intended to require the observation of limitations, or verification of information, not readily accessible to the relying party. Such a situation may need to be dealt with by the law applicable outside the Model Law. More generally, the consequences of failure by the relying party to comply with the requirements of article 11 are governed by the law applicable outside the Model Law (see A/CN.9/484, para. 75).

References to UNCITRAL documents

A/CN.9/484, para. 75;
A/CN.9/WG.IV/WP.88, annex, paras. 143-146;
A/CN.9/467, paras. 130-143;
A/CN.9/WG.IV/WP.84, paras. 61-63;
A/CN.9/465, paras. 109-122 (draft articles 10 and 11);
A/CN.9/WG.IV/WP.82, paras 56-58 (draft articles 10 and 11);
A/CN.9/457, paras. 99-107;
A/CN.9/WG.IV/WP.80. paras. 20-21.

Article 12. Recognition of foreign certificates and electronic signatures

(1) In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had to:

(a) the geographic location where the certificate is issued or the electronic signature created or used; or

(b) the geographic location of the place of business of the issuer or signatory.

(2) A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

(4) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

(5) Where, notwithstanding paragraphs (2), (3) and (4), parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

General rule of non-discrimination

152. Paragraph (1) is intended to reflect the basic principle that the place of origin, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective. Determination of whether, or the extent to which, a certificate or an electronic signature is capable of being legally effective should not depend on the place where the certificate or the electronic signature was issued (see A/CN.9/483, para. 27) but on its technical reliability.

"Substantially equivalent level of reliability"

153. The purpose of paragraph (2) is to provide the general criterion for the cross-border recognition of certificates without which suppliers of certification services might face the unreasonable burden of having to obtain licenses in multiple jurisdictions. For that purpose, paragraph (2) establishes a threshold for technical equivalence of foreign certificates based on testing their reliability against the reliability requirements established by the enacting State pursuant to the Model Law (ibid., para. 31). That criterion is to apply regardless of the nature of the certification scheme obtaining in the jurisdiction from which the certificate or signature emanated (ibid., para. 29).

Level of reliability varying with the jurisdiction

154. Through a reference to the central notion of a "substantially equivalent level of reliability", paragraph (2) acknowledges that there might be significant variance between the requirements of individual jurisdictions. The requirement of equivalence, as used in paragraph (2), does not mean that the level of reliability of a foreign certificate should be exactly identical with that of a domestic certificate (ibid., para. 32).

Level of reliability varying within a jurisdiction

155. In addition, it should be noted that, in practice, suppliers of certification services issue certificates with various levels of reliability, according to the purposes for which the certificates are intended to be used by their customers. Depending on their respective level of reliability, certificates and electronic signatures may produce varying legal effects, both domestically and abroad. For example, in certain countries, even certificates that are sometimes referred to as "low-level" or "low-value" certificates might, in certain circumstances (e.g., where parties have agreed contractually to use such instruments), produce legal effect (see A/CN.9/484, para. 77). Therefore, in applying the notion of equivalence as used in paragraph (2), it should be borne in mind that the equivalence to be established is between functionally comparable certificates. However, no attempt has been made in the Model Law to establish a correspondence between certificates of different types issued by different suppliers of certification services in different jurisdictions. The Model Law has been drafted so as to contemplate a possible hierarchy of different types of certificate. In practice, a court or arbitral tribunal called upon to decide on the legal effect of a foreign certificate would normally consider each certificate on its own merit and try to equate it with the closest corresponding level in the enacting State (A/CN.9/483., para. 33).

Equal treatment of certificates and other types of electronic signatures

156. Paragraph (3) expresses with respect to electronic signatures the same rule as set forth in paragraph (2) regarding certificates (ibid., para. 41).

Recognizing some legal effect to compliance with the laws of a foreign country

157. Paragraphs (2) and (3) deal exclusively with the cross-border reliability test to be applied when assessing the reliability of a foreign certificate or electronic signature. However, in the preparation of the Model Law, it was borne in mind that enacting States might wish to obviate the need for a reliability test in respect of specific signatures or certificates, when the enacting State was satisfied that the law of the jurisdiction from which the signature or the certificate originated provided an adequate standard of reliability. As to the legal techniques through which advance recognition of the reliability of certificates and signatures complying with the law of a foreign country might be made by an enacting State (e.g. a unilateral declaration or a treaty) the Model Law contains no specific suggestion (ibid., paras. 39 and 42).

Factors to be considered when assessing the substantial equivalence of foreign certificates and signatures

158. In the preparation of the Model Law, paragraph (4) was initially formulated as a catalogue of factors to be taken into account when determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph (2) or (3). It was later found that most of these factors were already listed under articles 6, 9 and 10. Restating those factors in the context of article 12 would have been superfluous. Alternatively, cross-referencing, in paragraph (4), the appropriate provisions in the Model Law where the relevant criteria were mentioned, possibly with the addition of other criteria particularly important for cross-border recognition, was found to result in an overly complex formulation (see, in particular, A/CN.9/483, paras. 43-49). Paragraph (4) was eventually turned into an unspecific reference to "any relevant factor", among which the factors listed under articles 6, 9 and 10 for the assessment of domestic certificates and electronic signatures are particularly important. In addition, paragraph (4) draws the consequences from the fact that assessing the equivalence of

foreign certificates is somewhat different from assessing the trustworthiness of a certification service provider under articles 9 and 10. To that effect, a reference has been added in paragraph (4) to "recognized international standards".

Recognized international standards

159. The notion of "recognized international standard" should be interpreted broadly to cover both international technical and commercial standards (i.e., market-driven standards) and standards and norms adopted by governmental or intergovernmental bodies (ibid., para. 49). "Recognized international standard" may be statements of accepted technical, legal or commercial practices, whether developed by the public or private sector (or both), of a normative or interpretative nature, which are generally accepted as applicable internationally. Such standards may be in the form of requirements, recommendations, guidelines, codes of conduct, or statements of either best practices or norms" (ibid., paras. 101-104).

Recognition of agreements between interested parties

160. Paragraph (5) provides for the recognition of agreements between interested parties regarding the use of certain types of electronic signatures or certificates as sufficient grounds for cross-border recognition (as between those parties) of such agreed signatures or certificates (ibid., para. 54). It should be noted that, consistent with article 5, paragraph (5) is not intended to displace any mandatory law, in particular any mandatory requirement for hand-written signatures that enacting states might wish to maintain in applicable law (ibid., para. 113). Paragraph (5) is needed to give effect to contractual stipulations under which parties may agree, as between themselves, to recognize the use of certain electronic signatures or certificates (that might be regarded as foreign in some or all of the States where the parties might seek legal recognition of those signatures or certificates), without those signatures or certificates being subject to the substantial-equivalence test set forth in paragraphs (2), (3) and (4). Paragraph (5) does not affect the legal position of third parties (ibid., para. 56).

References to UNCITRAL documents

A/CN.9/484, paras. 76-78;
A/CN.9/WG.IV/WP.88, annex, paras. 147-155;
A/CN.9/483, paras. 25-58 (article 12);
A/CN.9/WG.IV/WP.84, paras. 61-68 (draft article 13);
A/CN.9/465, paras. 21-35;
A/CN.9/WG.IV/WP.82, paras. 69-71;
A/CN.9/454, para. 173;
A/CN.9/446, paras. 196-207 (draft article 19);
A/CN.9/WG.IV/WP.73, para. 75;
A/CN.9/437, paras. 74-89 (draft article I); and
A/CN.9/WG.IV/WP.71, paras. 73-75.

Notes

[1] *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), paras. 223-224.

[2] Ibid., *Fifty-second Session, Supplement No. 17* (A/52/17), paras. 249-251.

[3] *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), paras. 223-224.

[4] Ibid., *Fifty-second Session, Supplement No. 17* (A/52/17), paras. 249-251.

[5] Ibid., *Fifty-third Session, Supplement No. 17* (A/53/17), paras. 207-211.

[6] Ibid., *Fifty-fourth Session, Supplement No. 17* (A/54/17), paras. 308-314.

[7] Ibid., *Fifty-fifth Session, Supplement No. 17* (A/55/17), paras. 380-383.

[8] This section is drawn from document A/CN.9/WG.IV/WP.71, part I.

[9] Numerous elements of the description of the functioning of a digital signature system in this section are based on the ABA Digital Signature Guidelines, p. 8 to 17.

[10] Certain existing standards such as the ABA Digital Signature Guidelines refer to the notion of "computational unfeasibility" to describe the expected irreversibility of the process, i.e., the hope that it will be impossible to derive a user's secret private key from that user's public key. "'Computationally unfeasible' is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance" (ABA Digital Signature Guidelines, p. 9, note 23).

[11] In situations where public and private cryptographic keys would be issued by the users themselves, such confidence might need to be provided by the certifiers of public keys.

[12] The question as to whether a government should have the technical ability to retain or recreate private confidentiality keys may be dealt with at the level of the root authority.

[13] However, in the context of cross-certification, the need for global interoperability requires that PKIs established in various countries should be capable of communicating with each other.